

FVR9416 SME Multi-WAN Firewall/VPN Router

操作安裝手冊

TW Version 1.3.0





Table of Contents





1. Introduction

FVR9416 為一台符合 SME 等級經濟型,高效能整合型之全功能新一代設計之防火牆系統, 除了具備絕大多數寬頻市場適用的對外聯機能力外,還內建了 16 Port 10/100Mbps QoS 交換器,以滿足多數企業對防火牆的市場需求,FVR9416 提供了硬體 DMZ 埠口為防火牆的標準配備使用外,並且提供四個 WAN ports.此四個 WAN ports 不僅可以支援高效能網路自動負載平衡模式(Intelligent Balancer by auto mode),亦可針對特定使用者的 IP 群組, 以提供分級服務 classes of service (CoS) (IP Group by Users).

配合新一代,多樣化之高安全整合性的防火牆設備需求環境,內建超高速的 Intel IXP 425 整合型 RISC CPU, 透過時脈 533Mhz 的高速處理架構下,發揮超高的網路效能,處理速度直逼中,大型企業用戶專用之昂貴防火牆設備;可符合企業界廣泛的應用系統支援,防火牆效能可達 200Mbps 以上,且具備支援目前企業廣泛應用之虛擬私有網路 VPN 硬體加速模式,包含 IPSec DES/3DES 等 VPN 加密,同時可以處理 200 條的 VPN 聯機,以 3DES 方式運作效能可達 70Mbps 以上,不論式功能面,實用安全性等,十足超越目前大型昂貴設備之規格.

FVR9416 IPSec VPN 適用於各辦公室, 事業夥伴及遠端使用者一個安全便利的網路加密方式. 包括 168 bit Data Encryption Standard (3DES), 56 bit Data Encryption Standard (DES), 以及 AH/ESP 方式. VPN 功能提供了各分支點間或大多數遠端使用者采 VPN 方式將資料自動加密解密的通訊方式,支援 Gateway To Gateway ,Client To Gateway 與 Group VPNs 等模式

FVR9416 內建進階型防火牆功能,能夠阻絕大多數的網路攻擊行為, 使用了 SPI 封包主動偵測檢驗技術 (Stateful Packet Inspection),封包檢驗型防火牆主要運作在網路的層級，但是藉由執行對每個連結的動態檢驗，也擁有應用程式的警示功能，讓封包檢驗型防火牆可以拒絕非標準的通訊協定所使用的連結, 預設自動偵測並阻擋. FVR9416 亦同時支援使用網路位址轉換 Network Address Translation (NAT)功能以及 Routing 路由模式,使網路環境架構更為彈性,易於規劃管理.

Content Filtering 內容過濾功能允許企業內部自訂網路存取規則,管理頁面內建可新增移除的過濾名單,可讓管理者選擇應該禁止存取或記錄監控哪些種類的網站, 如此可對學校或企業的 Internet 管理有明確的策略.自定過濾設定; 透過完整的 OS 管理核心. FVR9416 提供線上多樣化的日誌(SysLog)紀錄,支援線上管理設定工具, 可清楚易懂的網路設定組態、並加強管理全部的網路安全存取政策、VPN、及其它服務等.



FVR9416 能充分保障各型分支機構辦公室及各點間通訊的安全，避免日益趨多的商業機密竊取與攻擊破壞等.專屬的 OS 獨立式作業平臺，使用者無須具備專業級的網路知識即可易於安裝使用．透過流覽器如:IE, Netscape..來使用設定與管理 FVR9416 防火牆..

2. Main features: 主要產品功能

Product Features

網路聯機:

- One IP address to access the Internet over your entire network
- WAN: DHCP client, static IP, PPPoE
- DMZ: DHCP client, static IP, PPPoE
- LAN: DHCP auto-assignment, Mac-assignment DHCP static IP, Static IP.

Multi-WAN:

- 全自動型的負載平衡模式 Intelligent Bancer (Auto Mode)
- 網路服務偵測-NSD for Intelligent Balancer
- 特定使用者的 IP 群組，以提供分級服務 classes of service (CoS) (IP Group by Users)
- 協議綁定 Protocol Binding
- 服務品質 QoS

TCP/IP通訊協定:

- DHCP Client/Server
- PPPoE
- NAT with popular ALG support
- NAT with port forwarding
- NAT with port triggers
- DNS 轉送功能-DNS Relay
- ARP
- ICMP
- FTP/TFTP
- 密碼保護-Password protected configuration or management sessions for web access
- 全自動型的負載平衡模式 Intelligent Bancer (Auto Mode)
- 特定使用者的 IP 群組，以提供分級服務 classes of service (CoS)
- 以埠口為基礎的頻寬政策 Port-based QoS

- 時間伺服器通訊協定 NTP Time Server

路由通訊協定:

- 支援動態路由 RIP 1, RIP 2 compatible, 靜態路由 Static routing
- 支援閘道器模式 Gateway/路由模式 Routing Mode Support

路由器管理功能:

- 網頁模式管理與政策設定-Comprehensive web based management and policy setting
- 支援網路管理通訊協定 SNMP v1/v2c
- 線上動態即時系統日誌 Monitoring, Logging, 系統告警功能 Alarms of system activities
- 具備由 Web 方式的韌體升級備份(Fault-tolerance Web upgrade new software)
- 具備雙份的可置換韌體儲存空間備份(Dual Firmware Backup or Restore)
- Supports filter capability (Service and IP)
- 支援系統日誌以及電子郵件自動告警功能(Support Syslog & E-Mail Alert.)

防火牆功能:

- 防火牆主動封包檢測技術-Stateful Packet Inspection Firewall
- IP 位置過濾功能-IP filtering; allows you to configure IP address filters
- 埠口位置過濾功能-Port filtering; allows you to configure TCP/UDP port filters
- 支援硬體式的 DMZ 獨立埠口-Support Hardware DMZ to protect your network
- 阻斷式攻擊-Denial of Service (DoS) prevention Dos attack prevention
- 網頁內容過濾機制-Inappropriate URL command line filter
- 可設定網路存取時間控制-Set Internet accessing time schedule
- 網路攻擊模式偵測-Syn Flooding/IP Spoofing/Win Nuke/Ping Of Death
-

VPN 虛擬私有網路功能:

- 支援高速 3DES VPN 聯機效能速率可達 70Mbps-IPSec VPN 3DES Throughput 70Mbps UP.
- 支援 VPN 聯機通道數 200 條-Support up to 200 VPN tunnels
- 支援 2 組群組 VPN 功能-Up to 2 Group VPNs support
- 簡單易懂的 VPN 設定與管理介面-Friendly VPN Tunnel Management
- 支援 IKE 功能-IKE : Pre-Shared keys
- 支援 IPSec 標準的 DES/3DES 加密-IPSec Encryption DES/3DES
- 支援以 IPSec 為標準的 MD5/SHA1 驗證-IPSec Authentication MD5/SHA1
- 支援 PMTU 的密鑰管理-Support PMTU Key management: IKE
- 支援網功能變數名稱稱轉換 IP 位置 DNS Resolve



- 支援 PPTP 協定建立 VPN 通道
- 支援 VPN 透通功能-VPN Pass-through

其他功能:

- 虛擬主機 Virtual Server –Port Forwarding.
- 特殊應用軟體 Port-Triggering Support
- 支援內建軟體式非軍事管制區 DMZ 功能-Support Software DMZ.
- 支持國際標準即插即用功能-UPnP Support
- 支援一對一的網路位置轉譯功能-One to One NAT Support.
- 動態 DNS 支援-DDNS Support
- 可變更的 WAN 網路實體位置-MAC Clone Change Support
- 線上對外線路測試功能-Diagnostic with DNS Lookup & Ping.
- 路由器參數設定備份或是儲存-Setting Backup with Import & Export.

封包傳輸效能:

- 防火牆效能-Firewall: 200Mbps
- VPN 虛擬私有網路效能-3DES 168bit VPN: Up to 70Mbps.

硬體規格:

- 中央處理器 CPU: Intel IXP425- 533Mhz RISC
- 記憶體 SDRAM : 64Mbyte
- 快閃記憶體 Flash Memory: 16Mbyte

網路支援通訊規格:

- IEEE 802.3 10Base-T
- IEEE 802.3u 100Base-TX

網路實體介面規格:

- 廣域網路 WAN 1~4: Four 10/100Base-T/TX RJ-45 ports
- DMZ: One 10/100Base-T/TX RJ-45 ports
- 區域網路-LAN 1~11: 11 Port 10/100Base-T/TX RJ-45 ports
- 一個硬體重置按鈕可回復出廠預設值-One reset button for factory default setting

LED顯示:

- 系統-電源與自我檢測功能 System: Power, DIAG

- 速度 Speed, 聯機/動作 Link/Activity, 網際網路 WAN,連結 Connect

操作環境:

- 工作溫度Operating Temperature: 0^0 ~ 45^0C (32^0 ~ 113^0F)
- 儲存溫度Storage Temperature: -20^0 ~ 60^0C (-4^0 ~ 140^0F)
- 濕度 Humidity: 0 ~ 90% non-condensing

安規驗證:

- EMI/EMC: FCC Class A, CE Mark

外型尺寸:

- 13" (L) x 9" (W) x 1.75" (H) Inch

電源供應:

- Internal: AC100~240V /50~60Hz

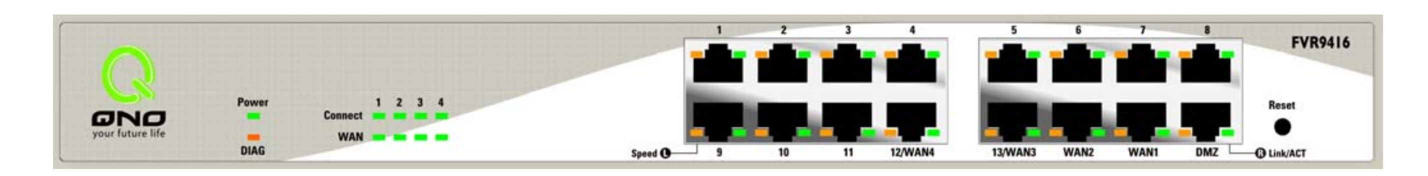
安裝方式:

- Desktop
- 19" Rack- Mount Tools Kit

3. How To Install FVR9416 如何安裝

Hardware 硬體安裝介紹

FVR9416 前面板



LED Status-面板燈號

LED	Color	Description
Power-電源	綠燈	綠燈亮: 電源開啟連接
DIAG-自我測試	橘燈	橘燈亮: 系統尚未完成開機自我檢測功能. 橘燈熄滅: 系統已經正常完成開機自我檢測功能.
Link/Act-聯機/動作	綠燈	綠燈亮: 乙太網路聯機正常 綠燈閃爍: 乙太網路埠口正在傳送/接收封包資料傳輸
Speed-速度	黃燈	黃燈亮: 乙太網路聯機在 100Mbps 的速度 黃燈熄滅: 乙太網路聯機在 10Mbps 的速度
WAN-網際網路	綠燈	綠燈亮: 指定為網際網路埠口 綠燈熄滅:指定為區域網路埠口
Connect-連結	綠燈	綠燈亮:當 WAN 端聯機並取得 IP 位置. 綠燈熄滅:當 WAN 端聯機並未取得 IP 位置

Reset Button 硬體 Reset 按鈕

Action	Description
按下 **Reset** 按鈕 **5** 秒	熱開機,重新啟動 FVR9416 DIAG 燈號: 紅色燈號慢慢閃爍
按下 **Reset** 按鈕 **10** 秒以上	回復原出廠預設值(Factory Default) DIAG 燈號: 紅色燈號快閃.



Replacing a Lithium Battery 更換系統內建電池

FVR9416 防火牆路由器內建有系統時間的電池. 此電池使用壽命約為 1~2 年. 當電池已經無法充電或是使用壽命到達後, FVR9416 將無法正確紀錄時間或是連接網際網路的同步 NTP 時間伺服器,您必須與您的系統廠商聯繫,以便取得更換電池的技術.

Note: 請勿自行拆解機器,若您需要更換電池的話,請與我們聯繫.

Setting up the Chassis-將 FVR9416 安裝於標準 19”機架上

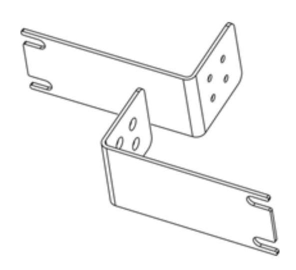
您可以將 FVR9416 放置於桌上使用,或是您有機房專用 19 吋標準機架的話,可以將 FVR9416 安裝於機架上,每一台 FVR9416 都有配備專用連接機架配件.

Setting the Chassis on a desktop or other flat, secure surface

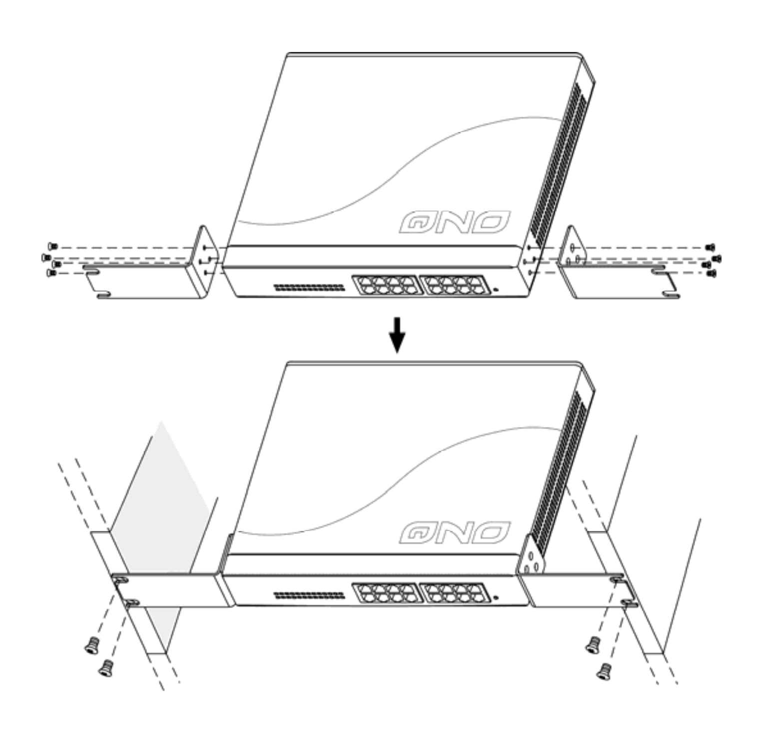
若您需要安裝 FVR9416 於機架上的話,請不要將其他過重的物品堆疊或是放置於機器上,以免因承受重量過重而發生危險或是損傷機器本體.

Rack-Mounting the Chassis

每一台 FVR9416 都有配備專用連接機架配件,包含 2 只 brackets 以及八顆專用螺絲提供與 FVR9416 連接安裝使用.

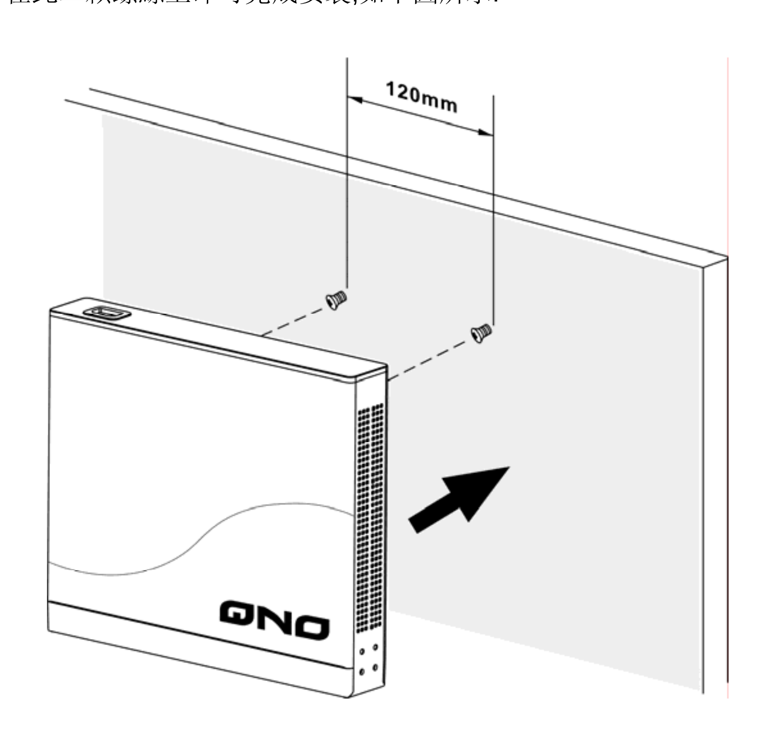


當您安裝鎖定 FVR9416 所提供的機架專屬配件後,您可以直接安裝於您的標準機架上,如下圖所示:



Wall-Mounting the Chassis-將 FVR9416 設備安裝在牆上

於 FVR9416 機器底部有二個十字孔位,您可以使用一般螺絲先旋轉鎖進牆壁上,確認牢固後,再將 FVR9416 的底部二個十字孔位準確的掛在此二顆螺絲上即可完成安裝,如下圖所示:





Connecting the FVR9416 to your Network-連接路由器到您的網路上

以下架構為如何連接 FVR9416 防火牆路由器到您的網路上,連接模式有分為二種:.

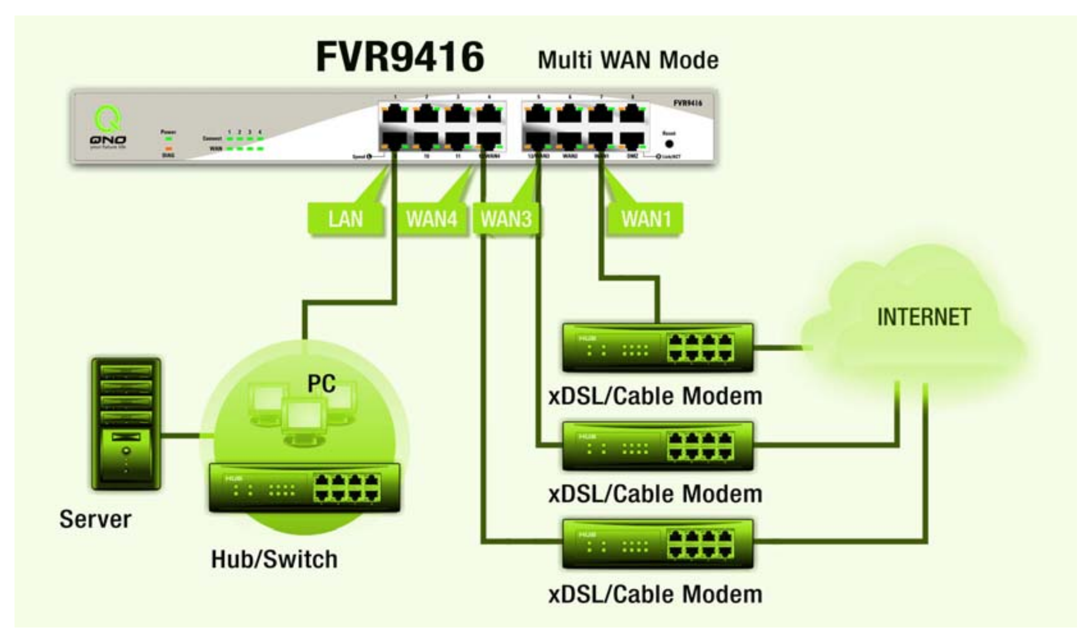


Figure 1: Multi WAN 負載平衡模式

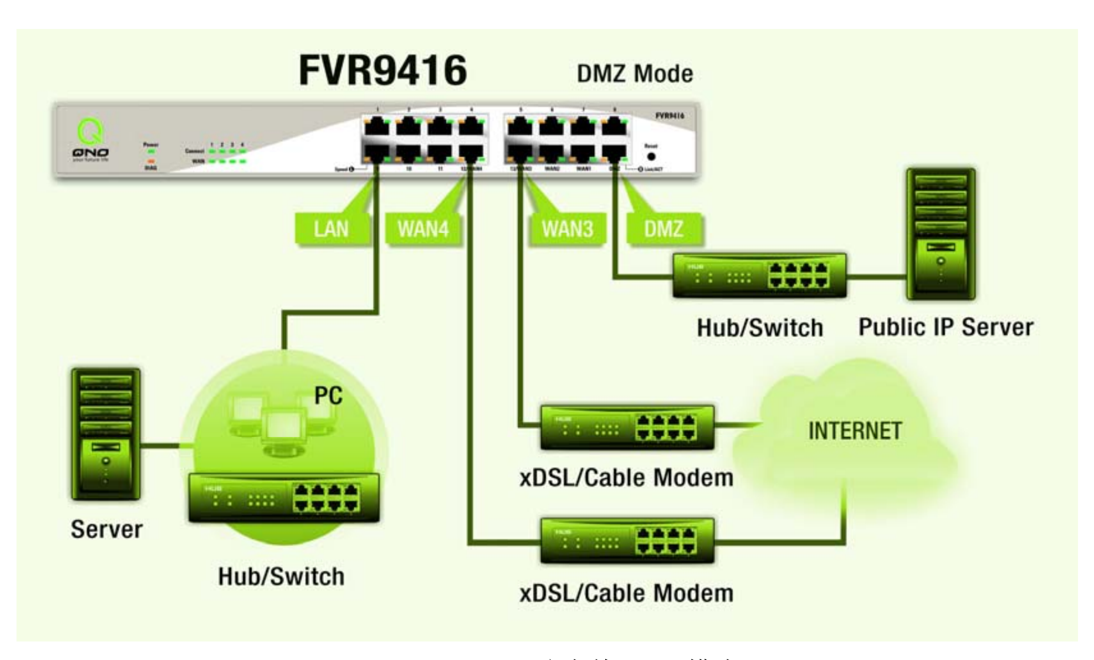


Figure 2: 防火牆 DMZ 模式 Z

FVR9416 防火牆路由器到您的網路上,連接模式有分為以下二種:

設定廣域網路聯機(**WAN** connection): WAN 埠口可以連接如 xDSL Modem, Switch HUB 或是外部路由器.



設定區域網路聯機(**LAN** connection): LAN 埠口可以連接如 Switch HUB 或是直接與 PC 聯機.

設定 **DM** 埠口: 此埠口可以連接如外部合法 IP 位置的伺服器, 如網頁 (Web) 以及電子郵件伺服器(Mail servers)等..

接下來請連接 FVR9416 背部電源線,然後會看到 FVR9416 的面板 Power 燈號亮起,以及一小段時間做自我開機測試即可開始使用並進行設置工作!

4. How To Manage FVR9416

Login 開始登入設定 FVR9416



請輸入使用者名稱(User Name)與密碼(Password)于上方所示密碼驗證欄位當中, 然後按下"確定"按鈕.

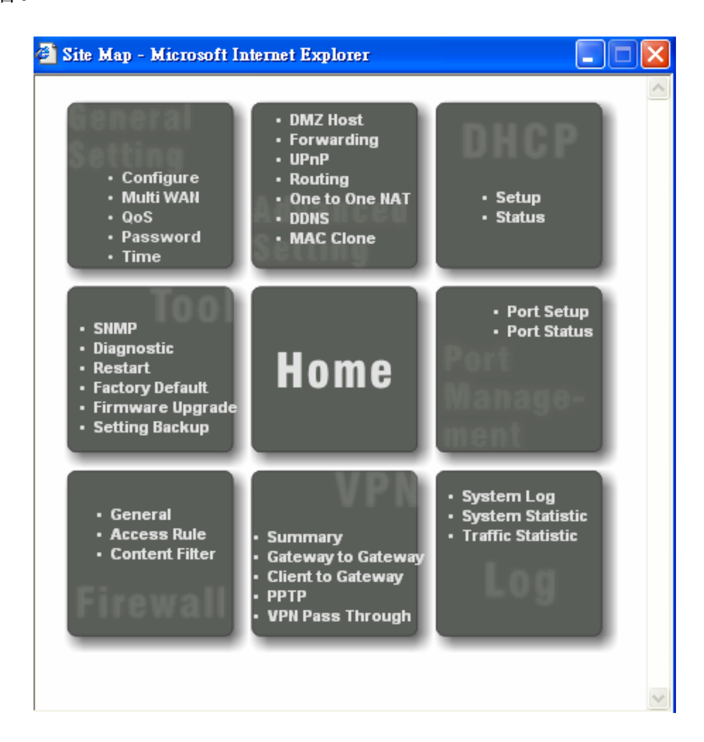
FVR9416 防火牆路由器其預設的使用者名稱(User Name)與使用者密碼(Password)皆為'admin' ,您可以於稍後設定時,更改此登入密碼!我們強烈建議您務必更改管理密碼!!



Sitemap

網頁設定項目地圖總表

按下"Sitemap"按鈕,可以顯示如下圖 FVR9416 的所有設定內容專案地圖總表(**Sitemap**),可以提供您快速的找到需要設定的專案以及內容.



Home 設定首頁

此首頁畫面(Home)顯示 FVR9416 防火牆路由器目前系統所有參數以及狀態顯示資訊,此資訊僅提供管理者讀取. 若您想進一部查詢該細部相關設定的話,可以按下各系不選向前端之超連結按鈕,並可以快速立即進入該選項設定當中.

System Information





Serial Number:(機器序號)

此為顯示 FVR9416 的機器序號.

Firmware version:(韌體版本資訊)

此為顯示 FVR9416 的目前使用的韌體版本資訊.

CPU:

此為顯示 FVR9416 使用的 CPU 型號為 Intel IXP425-533Mhz.

DRAM:

此為顯示 FVR9416 使用記憶體(DRAM)為 64MB.

Flash:

此為顯示 FVR9416 使用快閃記憶體(Flash)為 16MB.

System active time:

此為顯示 FVR9416 目前已經開機的時間.

Current time:

此為顯示 FVR9416 目前正確時間,但是必須注意,您需要正確設定與遠端 NTP 伺服器的時間同步後才會正確顯示..

Port Statistics(硬體各埠口-Port 狀態即時顯示)

Port Statistics

Port ID	1	2	3	4	5	6	7	8
Interface	LAN	LAN	LAN	LAN	LAN	LAN	LAN	LAN
Status	Connected	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled

Port ID	9	10	11	12	13	14	15	DMZ
Interface	LAN	LAN	LAN	WAN4	WAN3	WAN2	WAN1	DMZ
Status	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Connected	Enabled

在此畫面會顯示系統各埠口(Port)目前即時狀態顯示,包含每一個 Port (Connected-已經連接, Enabled-開啟, Disabled-關閉) . 使用者可以按下此狀態按鈕,查看各埠口更詳細的資料顯示. 於 **summary** table 總表, 會顯示目前該埠口設定狀態如, 網路連接 Link (up or down), 埠口 Port 開啟或關閉 Disable(on or off), 高低優先權 Priority (高 High or 一般 Normal), 連接速率 Speed Status(10Mbps or 100Mbps), 工作模式 Duplex Status(半雙工 half or 全雙工 full), 乙太網路自動偵測 Auto negotiation(Enabled or Disabled). 於此專案表格中(**statistics** table), 他將會顯示此埠口的接收 receive/傳送 transmit 的封包數以及 Byte 數/封包錯誤率等並計算總數量.

Port 1 Information - Microsoft Internet Explorer

Port1 Information

Summary:

Type	10Base-T / 100Base-TX
Interface	LAN
Link Status	Up
Port Activity	Port Enabled
Priority	Normal
Speed Status	100 Mbps
Duplex Status	Full
Auto negotiation	Enabled

Statistics:

Port Receive Packet Count	155549
Port Receive Packet Byte Count	33804474
Port Transmit Packet Count	229102
Port Transmit Packet Byte Count	246994709
Port Packet Error Count	0

Refresh Close

General Setting Status(一般設定狀態顯示)

General Setting Status

LAN IP :	192.168.1.1	
WAN1 IP :	192.168.5.178	Release Renew
WAN2 IP :	0.0.0.0	Release Renew
WAN3 IP :	0.0.0.0	Release Renew
WAN4 IP :	0.0.0.0	Release Renew
DMZ IP :	0.0.0.0	
Default Gateway (WAN1) :	192.168.5.1	
(WAN2) :	0.0.0.0	
(WAN3) :	0.0.0.0	
(WAN4) :	0.0.0.0	
DNS (WAN1) :	192.168.5.1 168.168.5.20	
(WAN2) :	192.168.5.1 192.168.5.2	
(WAN3) :		
(WAN4) :	192.168.5.1 192.168.5.2	
QoS (WAN1 | WAN2 | 3 | 4) :	Off | Off | Off | Off	

LAN IP: 此為顯示路由器的LAN端目前的IP位置設定資訊,系統預設為 192.168.1.1,並且可以按下該超連結直接進入該設定項目中.

WAN1~4 IP: 此為顯示路由器的WAN 1 端目前的IP位置設定資訊,並且可以按下該超連結直接進入該設定項目中.當使用者選擇自動取得IP位置時(**Obtain an IP automatically),** 他會顯示二個按鈕分別為釋放**-release** 與更新**-renew**. 使用者可以按下釋放- **release** 按鈕去做釋放ISP端所核發的IP位置,以及按下更新- **renew** 按鈕去做更新ISP端所核發的IP位置. 當選擇WAN端聯機使用如 **PPPoE** 或是 **PPTP**的話,他會變為顯示 連接-Connect 與中斷聯機-Disconnect.

DMZ IP: 此為顯示路由器的DMZ目前的IP位置設定資訊,並且可以按下該超連結直接進入該設定項目中.

Default Gateway: 此為顯示路由器的預設閘道IP位置設定資訊,並且可以按下該超連結直接進入該設定項目中

DNS: 此為顯示路由器的DNS(Domain Name Server)的IP位置設定資訊,並且可以按下該超連結直接進入該設定項目中..

QoS: It shows the QoS used in WAN1~4 and hyperlinks to QoS in General Setting page.

Advanced Setting Status(進階設定狀態顯示)

Advanced Setting Status

DMZ Host :	Disabled
Working Mode :	Gateway
DDNS (WAN1 | WAN2 | 3 | 4) :	Off | Off | Off | Off

DMZ Host: 此為顯示路由器的DMZ功能選項是否啟動,並且可以按下該超連結直接進入該設定項目中.系統預設此功能為關閉.

Working Mode: 此為顯示路由器的目前工作模式(可為NAT Gateway或是Router路由模式),並且可以按下該超連結直接進入該設定項目中.系統預設此功能為NAT Gateway模式.

DDNS(WAN1~4): 此為顯示路由器的DDNS動態DNS功能選項是否啟動,並且可以按下該超連結直接進入該設定項目中.系統預設此功能為關閉.

Firewall Setting Status(防火牆設定狀態顯示)

Firewall Setting Status

SPI (Stateful Packet Inspection) :	Off
DoS (Denial of Service) :	Off
Block WAN Request :	Off
Remote Management :	On

SPI (Stateful Packet Inspection): 此為顯示路由器是否開啟SPI(Stateful Packet Inspection)主動封包偵測過濾防火牆功能選項是否啟動(開啟-On/關閉-Off),並且可以按下該超連結直接進入該設定項目中.系統預設此功能為關閉-Off.

DoS (Denial of Service): 此為顯示路由器是否阻斷來自Internet 上的DoS攻擊功能選項,是否啟動(開啟-On/關閉-Off),並且可以按下該超連結直接進入該設定項目中.系統預設此功能為關閉-Off.

Block WAN Request: 此為顯示路由器是否阻斷來自Internet 上的ICMP-Ping 的回應功能選項,是否啟動(開啟-On/關閉-Off),並且可以按下該超連結直接進入該設定項目中.系統預設此功能為關閉-Off.

Remote Management: 此為顯示路由器的遠端管理功能選項是否啟動(開啟-On/關閉-Off),並且可以按下該超連結直接進入該設定項目中.系統預設此功能為關閉-Off

VPN Setting Status(VPN 設定狀態顯示)

VPN Setting Status

VPN Summary :	
Tunnel(s) Used :	0
Tunnel(s) Available :	200
No Group VPN was defined.	
PPTP Server :	Disabled

VPN Summary: 此為顯示路由器的VPN功能選項內容資訊,並且可以按下該超連結直接進入該設定項目中.

Tunnel(s) Used: 此為顯示路由器的 VPN 功能目前已經設定的 Tunnel 數量.

Tunnel(s) Available: 此為顯示路由器的 VPN 功能目前可使用的 Tunnel 數量..

Current Connected (The Group Name of GroupVPN1) users: 為顯示路由器的 VPN 1 目前線上使用 Tunnel 數量

Current Connected (The Group Name of GroupVPN2) users: 為顯示路由器的 VPN 2 目前線上使用 Tunnel 數量



若是 GroupVPN 為無設置的狀態,會顯示“No Group VPN was defined.”-沒有 GroupVPN 被設定的資訊..

PPTP server: It shows the status (Disabled/Enabled) of PPTP server and hyperlinks to PPTP page.

Log Setting Status: (系統日誌設定狀態顯示)

Log Setting Status

E-mail cannot be sent because you have not specified an outbound SMTP server address.

E-Mail 的超連結將會連到系統日誌設定畫面中:

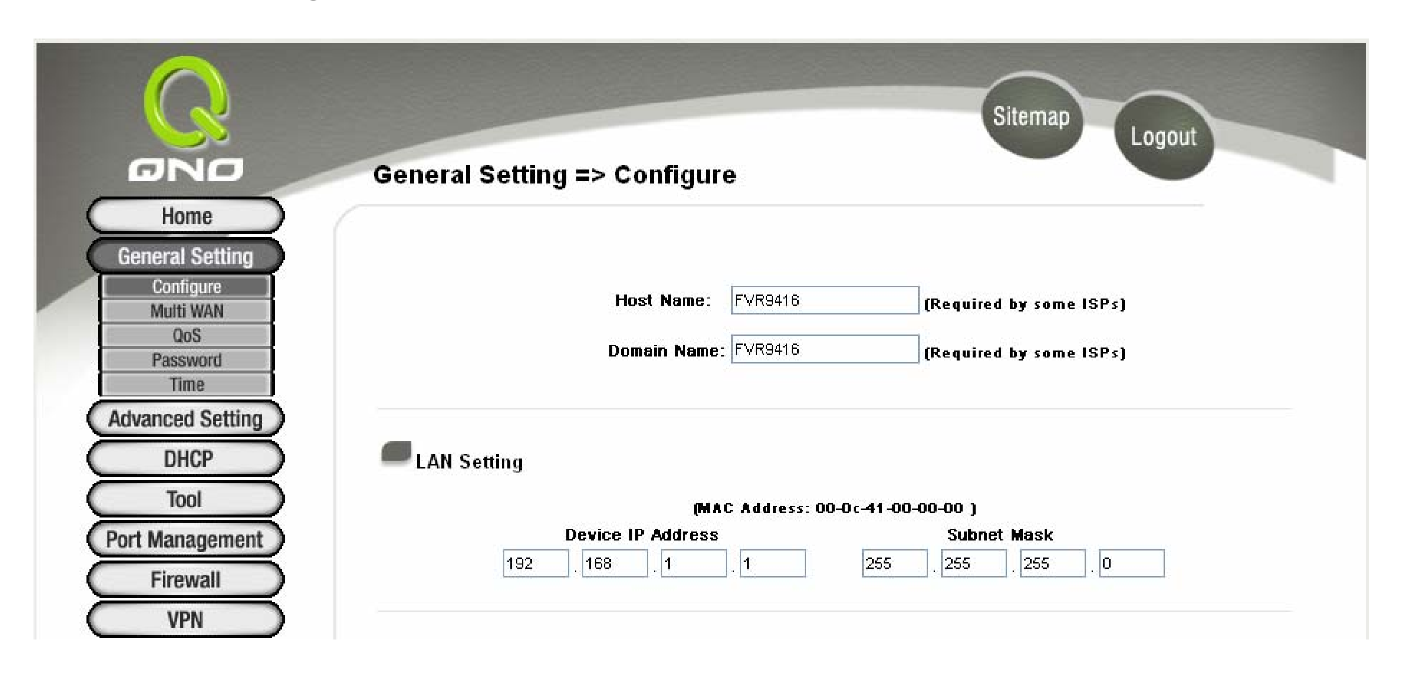
1.若您無設定電子郵件伺服器(Mail Server)于系統日誌設定中(Log page), 他將顯示您無設定電子郵件伺服器所以無法發送系統日誌電子郵件-“E-mail cannot be sent because you have not specified an outbound SMTP server address.”

2.若您已經設定電子郵件伺服器(Mail Server)于系統日誌設定中(Log page), 但是 Log 尚未達到設定傳送的條件時,它將顯示電子郵件伺服器已經設置-“E-mail settings have been configured.”

3.若您已經設定電子郵件伺服器(Mail Server)于系統日誌設定中(Log page), Log 也已經傳送出去時,它將顯示電子郵件伺服器已經設置,並且已經發送- “E-mail settings have been configured and sent out normally.”

4. 若您已經設定電子郵件伺服器(Mail Server)于系統日誌設定中(Log page), 但是 Log 無法正確傳送出去時,它將顯示電子郵件伺服器已經設置,但是無法傳送出去,可能是設定有問題-“E-mail cannot be sent out, probably use incorrect settings.”

General Setting 一般項目設定





此一般專案設定-General Setting 畫面為 FVR9416 防火牆路由器為基本的安裝設定內容. 對大多數的用戶來說,此預設的專案已經足夠連接網際網路而不需做任何變更. 當然有些情況下使用者需要一些 ISP 所提供的進一步詳細資訊.其詳細細部設定,請參考以下各節說明:

Configure 設定

Configure

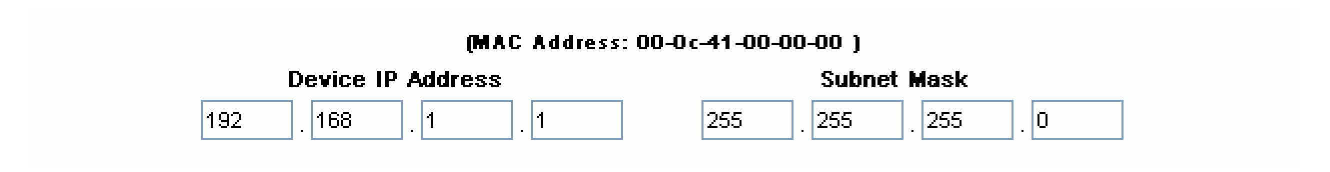
Host Name & **Domain Name**: 可輸入路由器的名稱-Host name 以及網功能變數名稱稱-Domain Name,於大多數的環境中不需做任何設定即可使用,國外有一些 ISP 可能需要用到!

Host Name: FVR9416 (Required by some ISPs)

Domain Name: FVR9416 (Required by some ISPs)

LAN Setting

此為顯示路由器的 LAN 端內部網路目前的 IP 位置設定資訊,系統預設為 192.168.1.1,子網路遮罩為 255.255.255.0.,可以依照您實際網路架構更動!.



WAN Setting



Please choose how many WAN ports you prefer to use : 4 (Default value is 4)

Interface	Connection Type	Config.
WAN1	Obtain an IP automatically	Edit
WAN2	Obtain an IP automatically	Edit
WAN3	Obtain an IP automatically	Edit
WAN4	Obtain an IP automatically	Edit

Please choose how many WAN ports you prefer to use 請輸入您要設定 WAN 埠口的數目,預設值為 4.您可以依照自己的需要加以更改.

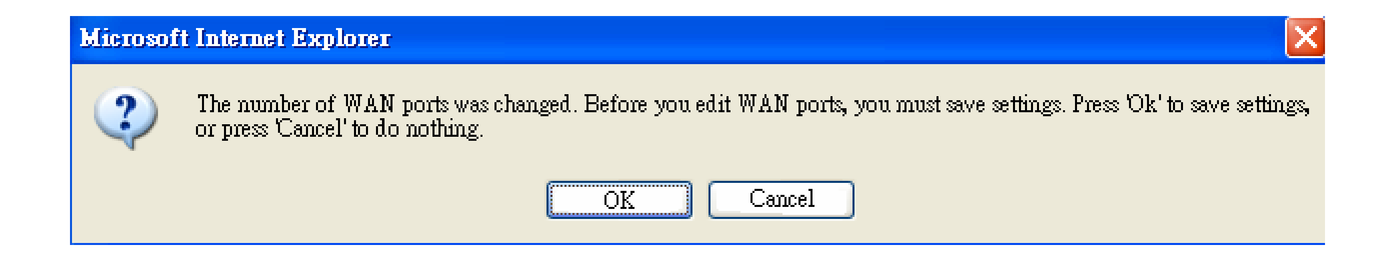
Interface: 顯示為第幾個 WAN 埠口

Connection Type 廣域網路 Internet 聯機型態設定:可以區分為四種.

Obtain an IP automatically:自動取得 IP 位置; Static IP: 固定 IP 位置聯機; PPPoE (Point-to-Point Protocol over Ethernet):PPPoE 撥號聯機; PPTP (Point-to-Point Tunneling Protocol): PPTP 撥號聯機



Config.: 顯示進一步更改設定:點選Edit進入近一步設定畫面



WAN Connection Type: 廣域網路 Internet 聯機型態設定

Obtain an IP automatically: 自動取得 IP 位置(常用在 Cable Modem 或是 DHCP Client 聯機型態上)
此為路由器系統預設的聯機方式,此聯機方式為 DHCP Client 自動取得 IP 模式,多為應用於如 Cable Modem 等連接,若您的聯機為其他不同的方式,請依照以下介紹並選取相關的設定.或是使用者自訂 DNS 的 IP 位置(Use the Following DNS Server Address),與此選項勾選並自訂填入 DNS 的 IP 位置.

Obtain an IP automatically

Use the Following DNS Server Addresses:

DNS Server (Required) 1: 0 . 0 . 0 . 0

2: 0 . 0 . 0 . 0

Use the Following DNS Server Address: 選擇使用自訂的 DNS 伺服器 IP 位置.

Domain Name Server (DNS): 輸入您的 ISP 所規定的名稱解析伺服器 IP 位置,最少頃填入一組,最多可填二組.

Static IP: 固定 IP 位置聯機

若您的 ISP 有核發固定的 IP 位置給您(如 1 個 IP 或是 8 個 IP 等),請您選擇此種方式聯機,將 ISP 所核發的 IP 資訊分別依照以下介紹填入相關設定參數中

Notes:請注意,有一些 ISP 雖會提供固定如一個 IP 位置給您,但是有可能是使用如 DHCP 自動取得 IP 或是 PPPoE 撥接取得一個固定 IP 模式,雖是每次都取得相同 IP 位置,但聯機模式您依然要選擇相關之模式才可!

Static IP

Specify WAN IP Address:	0	0	0	0
Subnet Mask:	0	0	0	0
Default Gateway Address:	0	0	0	0
DNS Server (Required) 1:	0	0	0	0
2:	0	0	0	0

Specify WAN IP Address: 輸入您的 ISP 所核發的可使用固定 IP 位置

Subnet Mask: 輸入您的 ISP 所核發的可使用固定 IP 位置的子網路遮罩,如:

發放 8 個固定 IP 位置:255.255.255.248
發放 16 個固定 IP 位置:255.255.255.240

Default Gateway IP Address: 輸入您的 ISP 所核發的可使用固定 IP 位置的預設通訊閘,若您是使用 ADSL 的話,一般說來都是 ATU-R 的 IP 位置.

Domain Name Server (DNS): 輸入您的 ISP 所規定的名稱解析伺服器 IP 位置,最少須填入一組,最多可填二組.

PPPoE (Point-to-Point Protocol over Ethernet): (Point-to-Point Protocol over Ethernet):PPPoE 撥號聯機

此項為 ADSL 計時制使用(適用於 ADSL PPPoE),填入 ISP 給予的使用者聯機名稱與密碼並以路由器內建的 PPP Over –Ethernet 軟體聯機,若是您的 PC 之前已經有安裝由 ISP 所給予的 PPPoE 撥號軟體的話,請將其移除,不需要再使用此個別連接網路。

PPPoE

User Name:

Password:

Connect on Demand: Max Idle Time 5 Min.

Keep Alive: Redial Period 30 Sec.

User Name: 輸入您的 ISP 所核發的使用者名稱

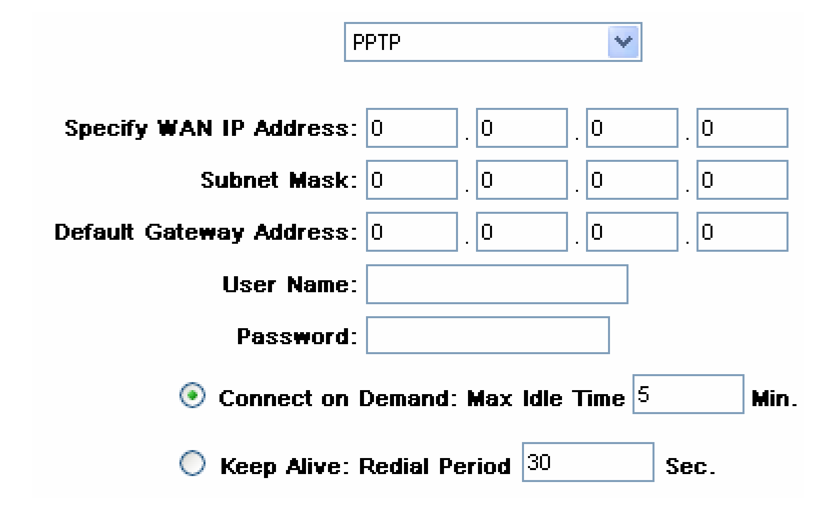
Password: 輸入您的 ISP 所核發的使用密碼

Connect-on-demand: 此功能能夠讓您的 PPPoE 撥接連線能夠使用自動撥號功能,當使用端若是有上網需求時,FVR9416 會自動向預設的 ISP 自動撥號聯機,當網路一段時間閒置無使用時,則系統會自動離線(自動離線無封包傳送時間預設為 5 分鐘).

Keep Alive: 此功能能夠讓您的 PPPoE 撥接連線能夠斷線自動重撥,而且可以自行設定重新撥接的時間,預設為 30 秒.

PPTP (Point-to-Point Tunneling Protocol): PPTP 撥號聯機

此項為 PPTP (Point to Point Tunneling Protocol) 計時制使用，填入 ISP 給予的使用者聯機名稱與密碼並以 FVR9416 內建的 PPTP 軟體聯機,(多為歐洲國家使用).



Specify WAN IP Address: 此項為設定固定 IP Address，設定的 IP 可由您的 ISP 所提供的位置輸入（此 IP 位置各 ISP 都於裝機後給予，請詢問您的 ISP 給予相關資訊）

Subnet Mask: 如上將 ISP 的子網路遮罩位址資料填入

Default Gateway Address: 輸入您的 ISP 所核發的可使用固定 IP 位置的預設通訊閘,若您是使用 ADSL 的話,一般說來都是 ATU-R 的 IP 位置.

User Name: 輸入您的 ISP 所核發的使用者名稱

Password: 輸入您的 ISP 所核發的使用密碼

Connect-on-demand: 此功能能夠讓您的 PPTP 撥接連線能夠使用自動撥號功能,當使用端若是有上網需求時,FVR9416 會自動向預設的 ISP 自動撥號聯機,當網路一段時間閒置無使用時,則系統會自動離線(自動離線無封包傳送時間預設為 5 分鐘).

Keep Alive: 此功能能夠讓您的 PPTP 撥接連線能夠斷線自動重撥,而且可以自行設定重新撥接的時間,預設為 30 秒.

DMZ Setting

于某些網路環境應用來說,您可能會需要用到獨立的 DMZ 非軍事管制區介面來置放您的對外服務伺服器,如 WWW 與 Mail 伺服器等; FVR9416 提供一組獨立的 DMZ 介面來設定連接於合法 IP 位置的伺服器.此 DMZ 介面為連接 Internet 與區域網路之間的溝通橋樑.

DMZ Setting

Interface	IP Address	Config.
DMZ	0.0.0.0	Edit

Interface: 顯示為 DMZ 埠口

IP Address: 顯示目前預設的網域網定固定 IP 位置資訊.預設值為 0.

Config. 顯示進一步更改設定:點選Edit進入近一步設定畫面.

Interface : DMZ

Specify DMZ IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Specify DMZ IP Address: 請輸入 DMZ 介面的 IP 位置資訊以及子網路遮罩.

請按下 **Back** 按鈕回到上一頁或是 **Apply** 按鈕儲存網路設定變更或是按下 **Cancel** 按鈕不做任何設定變更.

Multi WAN-多 WAN 埠配置

於多 WAN 的運作模式當中,提供了使用者二種模式選擇,分別為 **–全自動型的負載平衡模式 Intelligent Banancer(Auto Mode)** 以及 **特定使用者的 IP 群體模式 IP Group (By Users)**

全自動型的負載平衡模式 Intelligent Banancer(Auto Mode)的情況下

, 系統自動整合 WAN1 到 WAN4 四條線路最大頻寬做最佳的負載平衡.

General Setting => Multi WAN

Mode

◉ Intelligent Balancer (Auto Mode)

○ IP Group (By Users)

Interface Setting

Interface	Mode	Config.
WAN1	Auto	Edit
WAN2	Auto	Edit
WAN3	Auto	Edit
WAN4	Auto	Edit

Apply Cancel

Mode: 選擇全自動型的負載平衡模式 Intelligent Balancer (Auto Mode)

Interface Setting: 選擇要進一步設定的介面.

Interface: 顯示出網際網路埠口的數目,預設值為四個.

Mode: 在設定完後顯示的結果.在全自動型的負載平衡模式 Intelligent Balancer (Auto Mode)的情況之下,會自動顯示出自動分配頻寬 Auto.

Config.: 可經由點選 Edit 進行進一步的設定.

Apply: 按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數..

Cancel: 按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效



General Setting => Multi WAN

Interface : WAN1

The Max. Bandwidth provided by ISP : Upstream 512 Kbit/Sec Downstream 512 Kbit/Sec

Network service detection

Retry count 5

Retry timeout 30 second

When Fail Remove the Connection

Default Gateway

ISP Host

Remote Host

DNS Lookup Host

Interface: 顯示所選定的網際網路埠口 WAN 1.

The Max. Bandwidth provided by ISP: 可以自動填入要上傳(Upstream)或下載(Downstream)的網路流量.範圍介於 0~100Mbits 之間

Network Services Detection: 網路對外服務偵測機制.若勾選此項設定,則會出現 Retry Count,Retry Timeout..等以下的訊息.若沒有則沒有以下的訊息.

Retry Count: 對外聯機偵測重試次數,預設值為五次.若是於此設定次數當中,Internet 沒有回應的話,就是為對外線路中斷!

Retry Timeout: 對外聯機偵測逾時時間(秒),預設值為 30.秒.若是於此設定秒數當中,Internet 沒有回應的話,就是為對外線路中斷.

When Fail **(1)Generate the Error Condition in the System Log:在系統日誌中會產生錯誤訊息的資訊:** 當偵測到與 ISP 連結失敗時,系統就會在系統日誌中將這項錯誤訊息紀錄下來..
(2)Remove the Connection 忽略此項訊息: 當偵測到與 ISP 連結失敗時,系統不會在系統日誌中將這項錯誤訊息紀錄下來.原本在此 WAN 端的封包傳遞會自動轉換到其他預設成 Auto Mode 的 WAN 端.等到原本 WAN 端重新連結,則封包傳遞會自動轉換回來.

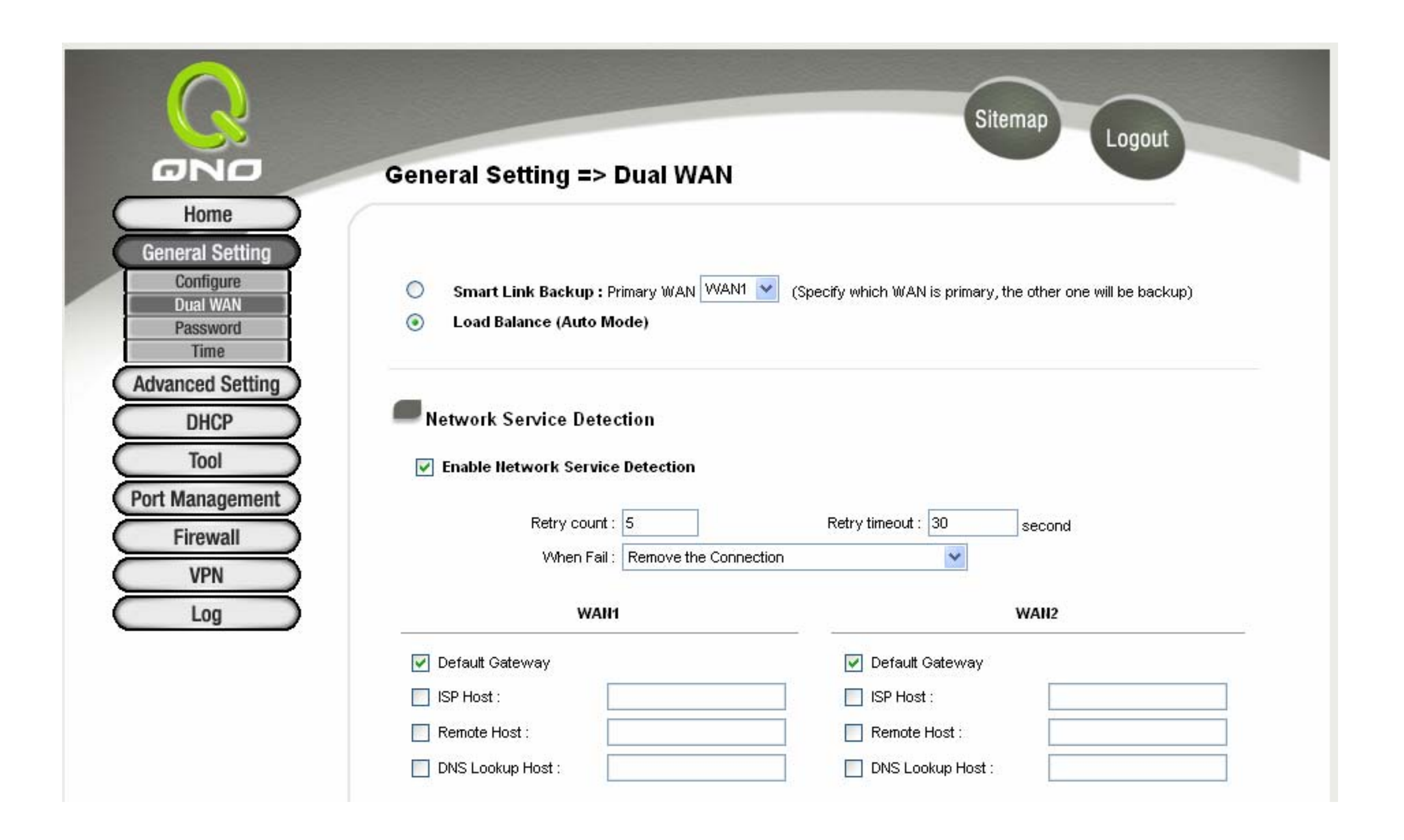
Default Gateway: 近端的預設通訊網關位置,如 ADSL 路由器的 IP 位置

ISP Host: ISP 端的偵測位置,如 ISP 的 DNS IP 位置等

Remote Host: 遠端的網路節點偵測位置.

DNS Lookup Host: 網功能變數名稱稱端 DNS 的偵測位置.





Protocol Binding -

它提供使用者可將特定的 IP 或/和特定的應用服務 Service 限定經由特定的 WAN port 出去,而其他的非特定的 IP 或/Service 也可走此 WAN



Protocol Binding

Service: SMTP [TCP/25~25]
Service Management
Source IP: 192 . 168 . 1 . 0 to 0
Distination IP: 0 . 0 . 0 . 0
Enable:
Add to list
Delete selected application
Back Apply Cancel

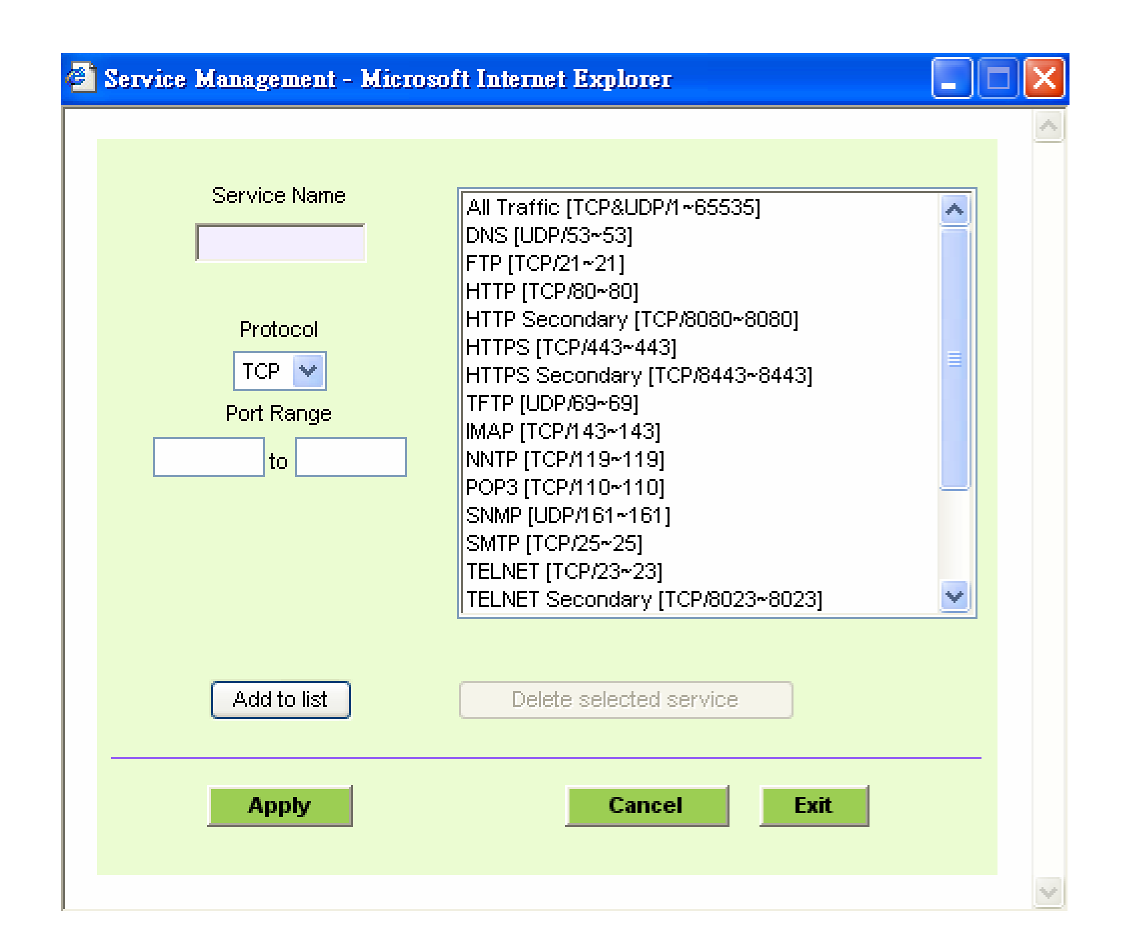
Service:	在此選擇欲開啟的虛擬主機的服務號碼預設列表(如 All(TCP&UDP)0-65535),如 WWW 為 80(80~80), FTP 為 21~21,可參考服務號碼預設列表!. 預設的 Service 為 SMTP。
Source IP:	使用者可以限定特定的內部虛擬 IP 位置的封包經由特定的介面 WAN port 出去。在此填上的內部虛擬 IP 位置範圍,如 192.168.1.100 到 150. 如果使用者只需要設定特定的而不需設定特定的 IP 的話，建議您在 IP 的欄位皆填入 0。
Destination IP:	在此填上的外部固定 IP 位置,如 210.11.1.1 使用者可以限定到哪一特定目的 IP 的封包經由特定的介面 WAN port 出去.在此填上的外部固定 IP 位置,如 210.11.1.1.如果使用者只需要設定特定的應用而不需設定特定的 IP 的話，建議您在 IP 的欄位皆填入 0.
Enable:	開啟此服務功能
Add to list:	新增或刪除管理服務埠號列表
Delete selected application:	增加到開啟服務專案內容
Back:	按下此按鈕”Back”即會回到上一頁
Apply:	按下此按鈕”Apply”即會儲存剛才所變動的修改設定內容參數..
Cancel:	按下此按鈕”Cancel”即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

以上服務表列,一些為較常使用的項目,若您預開啟的項目沒有在表列中,您可以使用 **Services Management:** 新增或刪除管理服務埠號列表功能達成,如以下所述



Service Management: 開啟埠號位置新增管理功能

Services Name:	在此自訂選擇欲開啟的服務埠號名稱加入列表中,如 Edonky 等
Protocol:	在此填上欲開啟的服務埠號的位置範圍,如 500~500 或是 2300~2310 等.
Port Range:	開啟此服務功能
Add to List:	增加到開啟服務專案內容列表,最多可新增 30 組.
Delete Selected Services:	刪除所選擇的開啟服務專案之一筆內容
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數..
Cancel:	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效
Exit:	離開此功能設定畫面



IP Group (By Users)IP 群組流量綁定功能

IP 群組功能啟動時可以讓管理者自行定義優先權以及每一個群組的指定通道出口.此功能可以讓網路帶寬可以以優先權方

式指定 IP.

Home
General Setting
Configure
Multi WAN
QoS
Password
Time
Advanced Setting
DHCP
Tool
Port Management
Firewall
VPN
Log

Sitemap Logout

General Setting => Multi WAN

Mode

○ Intelligent Balancer (Auto Mode)

⦿ IP Group (By Users)

Interface Setting

Interface	Mode	Config.
WAN1	Dispatched by system	Edit
WAN2	Dispatched by system	Edit
WAN3	Dispatched by system	Edit
WAN4	Dispatched by system	Edit

Apply Cancel

your future life

Mode: 使用者定義以 IP 群組方式來實現負載均衡模式.

Interface Setting: 使用者可以選擇不同的 WAN 埠來設定.

Interface: 這裏會顯示出有多少的 WAN 埠,預設為 4 個 WAN 埠.

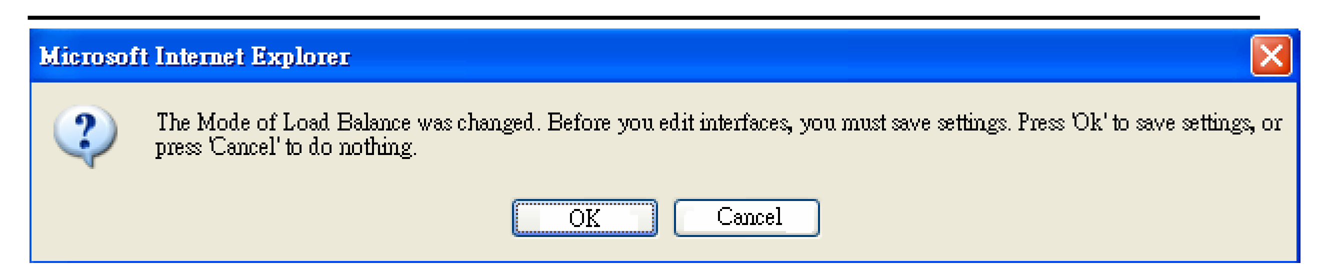
Mode: 於此會顯示設定後的訊息,當使用者設定每一個 WAN 埠後,此會顯示“Dispatched by user”的字樣. 如果沒有配置將會顯示“Dispatched by system”.

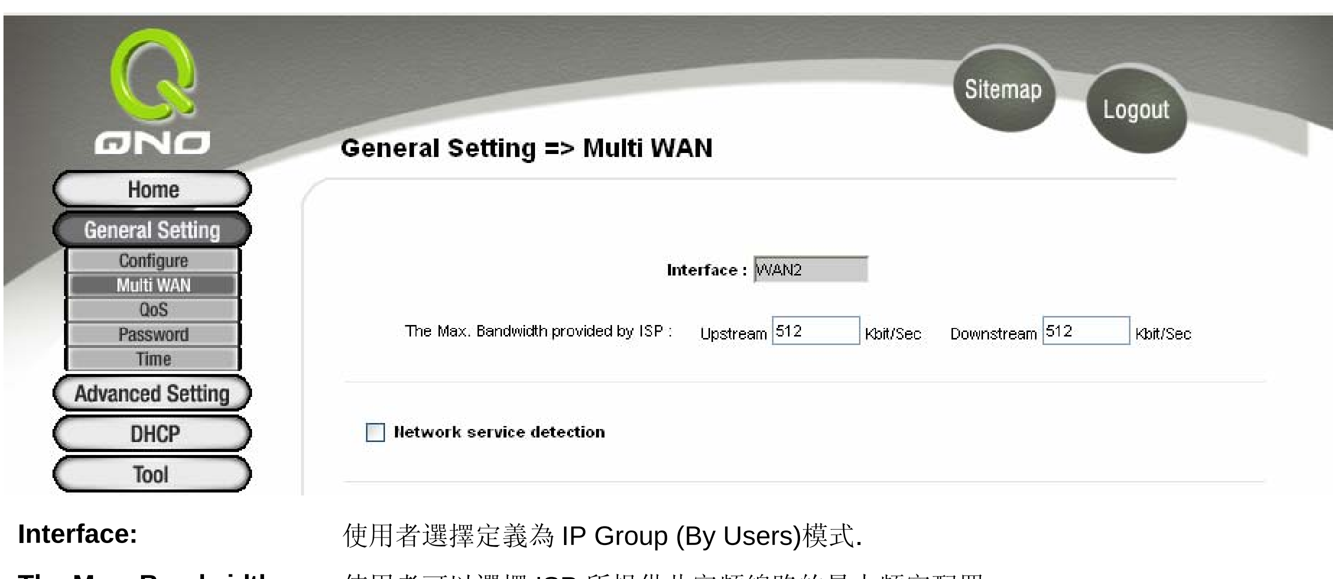
Config.: 按下 Edit 按鈕可以開始該介面埠配置.

Apply: 按下此按鈕”Apply”即會儲存剛才所變動的修改設定內容參數..

Cancel: 按下此按鈕”Cancel”即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

若是使用者想要變更使用模式從自動負載均衡 Intelligent Balancer (Auto Mode)到 IP 群組模式(By users),當按下 Edit 按鈕後,會顯示以下對話方塊訊息.





Interface: 使用者選擇定義為 IP Group (By Users)模式.

The Max. Bandwidth provided by ISP:: 使用者可以選擇 ISP 所提供此寬頻線路的最大頻寬配置

Network Service detection 對外網路服務偵測點配置.



IP Group
IP 群組功能啟動時可以讓管理者自行定義優先權以及每一個群組的指定通道出口.此功能可以讓網路帶寬可以以優先權方式指定 IP.

Services:
在此選擇欲開啟的虛擬主機的服務號碼預設列表(如 All(TCP&UDP)0-65535),如 WWW 為 80(80~80), FTP 為 21~21,可參考服務號碼預設列表!. 預設的 Service 為 SMTP

Services Management:
於服務表專案新增或是刪除.

Source IP:
使用者可以限定特定的內部虛擬 IP 位置的封包經由特定的介面 WAN port 出去。在此填上的內部虛擬 IP 位置範圍,如 192.168.1.100 到 150. 如果使用者只需要設定特定的而不需設定特定的 IP 的話, 建議您在 IP 的欄位皆填入 0.

Destination IP
在此填上的外部固定 IP 位置,如 210.11.1.1 使用者可以限定到哪一特定目的 IP 的封包經由特定的介面 WAN port 出去.在此填上的外部固定 IP 位置,如 210.11.1.1.如果使用者只需要設定特定的應用而不需設定特定的 IP 的話, 建議您在 IP 的欄位皆填入 0

Enable:
使用者可以選擇此按鈕開啟此條規則.

Delete selected application :
刪除所選擇的項目.

Add New:
重新配置一條新的規則.

Back:
按下此按鈕"Back"即會回到上ㄧ個畫面顯示

Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數..
Cancel:	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

Quality of Service (QoS)

FVR9416 提供使用者在特定的網際網路埠口上,提供流量速度控制 Rate Control 或者是服務優先性 Priority 等兩種服務品質 QoS 的設定類型,以滿足特定使用者的頻寬需求.使用者在此只能夠在這兩種設定類型選擇其中的一種作頻寬服務品質 QoS.

在選擇 Rate Control 的情況下

FVR9416 可以針對特定的網際網路埠口,保證在提供特定的服務,來源 IP 或者是目的 IP 時,有保障的頻寬,來傳送重要的資訊封包.

Enable:	啟動選擇要執行此 QoS 的網際網路埠口
Type:	點選流量速度控制 Rate Control
Service:	在此選擇欲開啟的虛擬主機的服務號碼預設列表(如 All(TCP&UDP)0-65535),如 WWW 為 80(80~80), FTP 為 21~21,可參考服務號碼預設列表!.
Services Management:	新增或刪除管理服務埠號列表
Direction:	可以選擇需要管制 Uplink (上傳流量) 或是 downlink (下載流量) 於上下的選擇按鈕上.
Minimum Rate (Min. Rate):	輸入保證/最小頻寬使用率,例如輸入 200 於控格中,即表示於此管制專案中將會保證有 200kbps/Sec 給予此頻寬政策條件內容符合的



Maximum Rate (Max. Rate):	輸入最大頻寬使用率,例如輸入 500 於控格中,即表示於此管制項目中最大的流量將會最大使用不超過 500kbps/Sec
Enable:	開啟此服務功能
Add to List:	增加到開啟服務專案內容列表.
Delete Selected Services:	刪除所選擇的開啟服務專案之一筆內容
Add New:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數..
Apply	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效
Cancel	開啟此服務功能

在選擇服務優先性 **Priority** 的情況下

FVR9416 可以針對特定的網際網路埠口,保證在提供特定的服務時,可以區分成高,中或低的優先順序,來傳送重要的資訊封包,其預設值為中優先性.

Enable:	啟動選擇要執行此 QoS 的網際網路埠口
Type:	點選**服務優先性 Priority**
Services:	在此選擇欲開啟的虛擬主機的服務號碼預設列表(如 All(TCP&UDP)0-65535),如 WWW 為 80(80~80), FTP 為 21~21,可參考服務號碼預設列表!.
Services Management:	新增或刪除管理服務埠號列表
Direction:	可以選擇需要優先權管制 Uplink (上傳流量) 或是 downlink (下載流量) 於上下的選擇按鈕上.
Priority:	在選擇服務的優先性時,使用者可以選擇高優先性 High(60%) 與低優先性 Low(10%) 兩種.其餘部份則為中優先性(30%).
Add to List:	增加到開啟服務專案內容列表,最多可新增 30 組.
Enable:	開啟此服務功能
Delete Selected application:	刪除所選擇的開啟服務專案之一筆內容
Add New:	重新新增一條新的條例
Apply	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數..
Cancel	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

在此選擇欲開啟的虛擬主機的服務號碼預設列表(如 All(TCP&UDP)0-65535),如 WWW 為 80(80~80), FTP 為 21~21,可參考服務號碼預設列表!. 預設的 Service 為 SMTP

Password

本功能設定多為 FVR9416 的進階管理專案- 管理者密碼設定，本機使用密碼出廠值為“admin”，您可當設定完成後修改此一存取密碼，但是記得設定完成後 Apply！.



Sitemap
Logout
General Setting => Password
Home
General Setting
Configure
Dual WAN
Password
Time
Advanced Setting
DHCP
Tool
Port Management
Firewall
VPN
Log
User Name: admin
Old Password:
New Password:
Confirm New Password:
Apply
Cancel
your future life

User Name:	預設為 admin
Old Password:	填寫原本舊密碼
New Password:	填寫所更改密碼
Confirm New Password:	再填寫確認一次更改密碼
Apply	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數..
Cancel	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

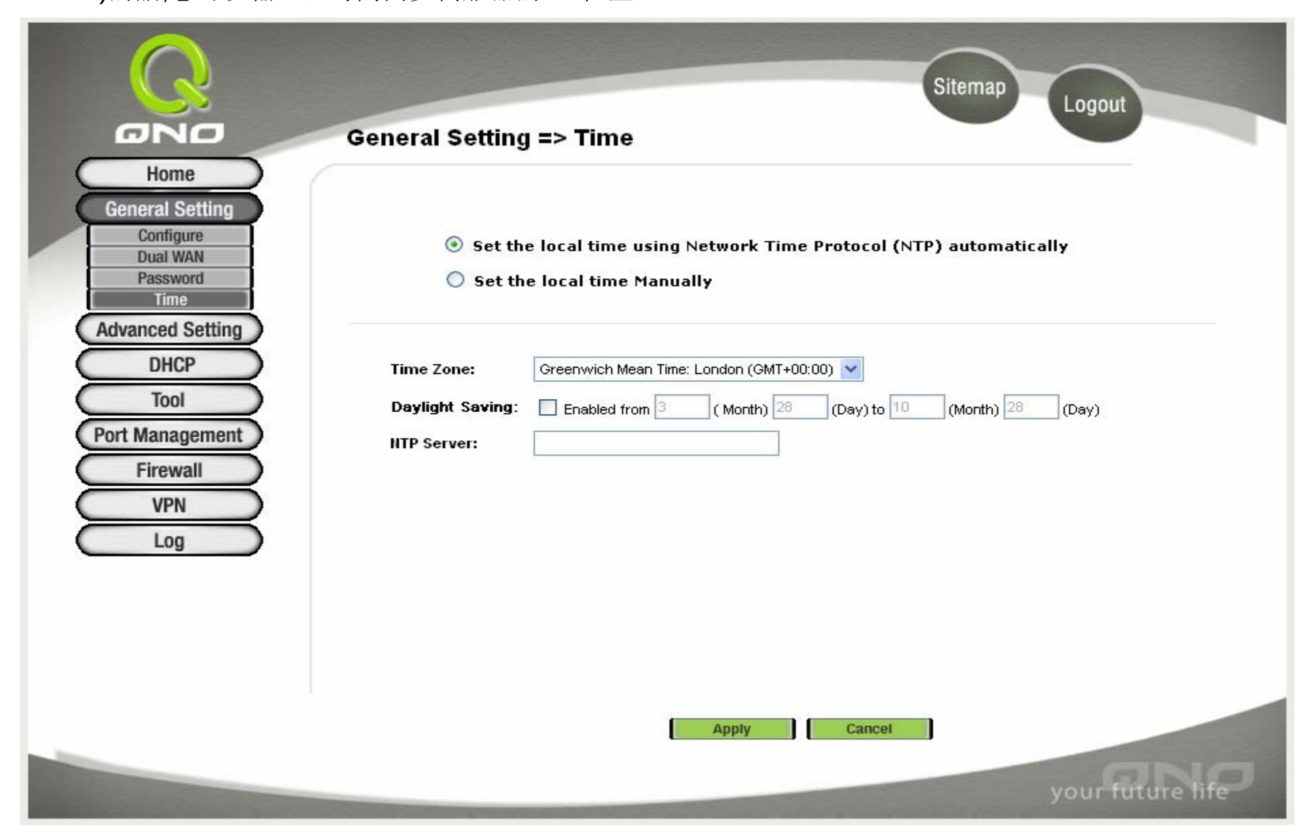
.

Time 系統時間設定

FVR9416 使用了正確的時間計算功能,您可以選擇與 FVR9416 內建的外部時間同步伺服器(NTP Server)或是自己設定正確時間參數,此項參數設置可以讓您在看 FVR9416 的系統紀錄,或是設置網路存取時間功能時,可以正確的瞭解事件發生正確時間以及關閉存取或是開放存取 Internet 資源的依據條件.

Automatically: 設定自動與網路上的 NTP 伺服器同步時間

請於 Time Zone 選項選擇您所在區域的時間參數以及日光節約時間,或是您有專屬使用的時間同步伺服器(NTP Server)的話,您可以輸入此時間同步伺服器的 IP 位置.



Manually: 手動輸入日期時間參數

於此輸入正確小時(Hours), 分鐘(Minutes), 秒(Seconds), 月份(Month), 日(Day) 與年(Year).

Sitemap
Logout
General Setting => Time
Home
General Setting
Configure
Dual WAN
Password
Time
Advanced Setting
DHCP
Tool
Port Management
Firewall
VPN
Log

○ Set the local time using Network Time Protocol (NTP) automatically
◉ Set the local time Manually

6 Hours 19 Minutes 29 Seconds
8 Month 27 Day 2004 Year

Apply Cancel

your future life

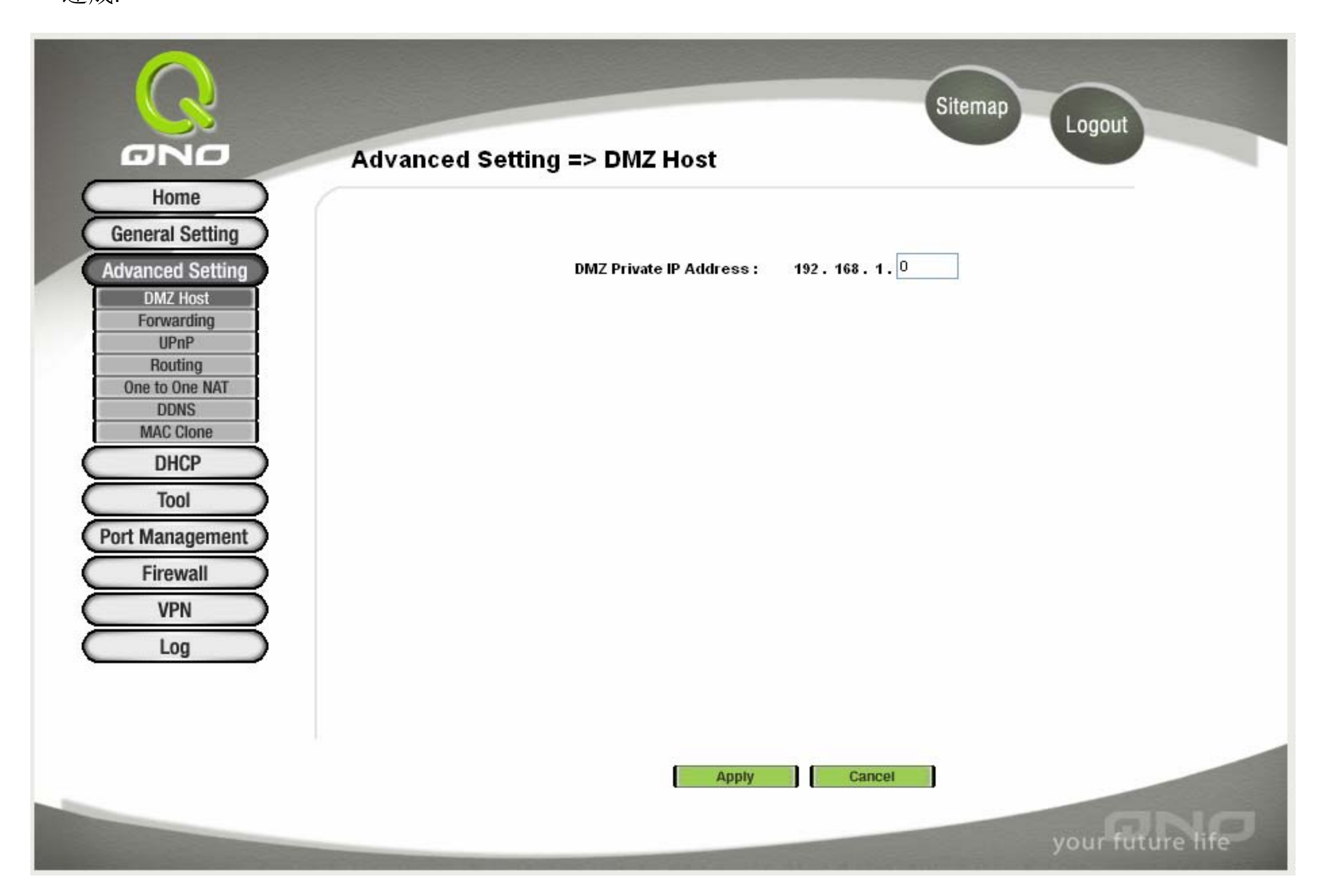
按下此按鈕”Apply”即會儲存剛才所變動的修改設定內容參數. 按下”Cancel”即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效.



Advanced Setting

DMZ Host-(Demilitarized Zone)

當您使用 NAT 模式運作時,有時需要使用如“網路遊戲”等任何不支援虛擬 IP 位置的各種應用程式時,可將 FVR9416 的 WAN Port 的合法 IP 位置直接對應內部虛擬 IP 位置使用,設定如下填入下方的設定可用此功能達成.



於選擇 **“DMZ Host”** 功能時,若您要取消此功能必須於後面設定虛擬 IP 位置地方填入**“0”** 的參數,才會停止此功能使用.

按下此按鈕”Apply”即會儲存剛才所變動的修改設定內容參數. 按下”Cancel”即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效.

Forwarding

Port forwarding 虛擬主機架設，若是網路中含有伺服器功能（意指對外部的服務主機 WWW,FTP．Mail 等）可將此主機利用防火牆功能，將主機視為一虛擬的位置，可用 FVR9416 的外部合法 IP 位置<Public IP>，經過 port 的轉換，（如 WWW 為 port 80），直接存取內部伺服器的服務。若於設定畫面中，選項填入ＷＷＷ伺服器位置，如 192.168.1.50 且 port 是 80 的話，當 Internet 要存取這個網頁時只要鍵入：

http://211.243.220.43(此為 FVR9416 的外部合法 IP 位址)



此時，就會透過 FVR9416 的 Public IP 位置去轉換到 192.168.1.50 的虛擬主機上的 Port 80 讀取網頁了。

其他的服務設定，如同上一般；只要將所用的 Server 的 UDP Port 號碼，以及虛擬主機的 IP 位置填入即可！.



Services:	在此選擇欲開啟的虛擬主機的服務號碼預設列表(如 All(TCP&UDP)0-65535),如 WWW 為 80(80~80), FTP 為 21~21,可參考服務號碼預設列表!.
IP Address:	在此填上虛擬主機相對應的內部虛擬 IP 位置,如 192.168.1.100
Enable:	開啟此服務功能
Service Management:	新增或刪除管理服務埠號列表
Add to List:	增加到開啟服務專案內容

以上服務表列,一些為較常使用的項目,若您預開啟的項目沒有在表列中,您可以使用 **Services Management:** 新增或刪除管理服務埠號列表功能達成,如以下所述:

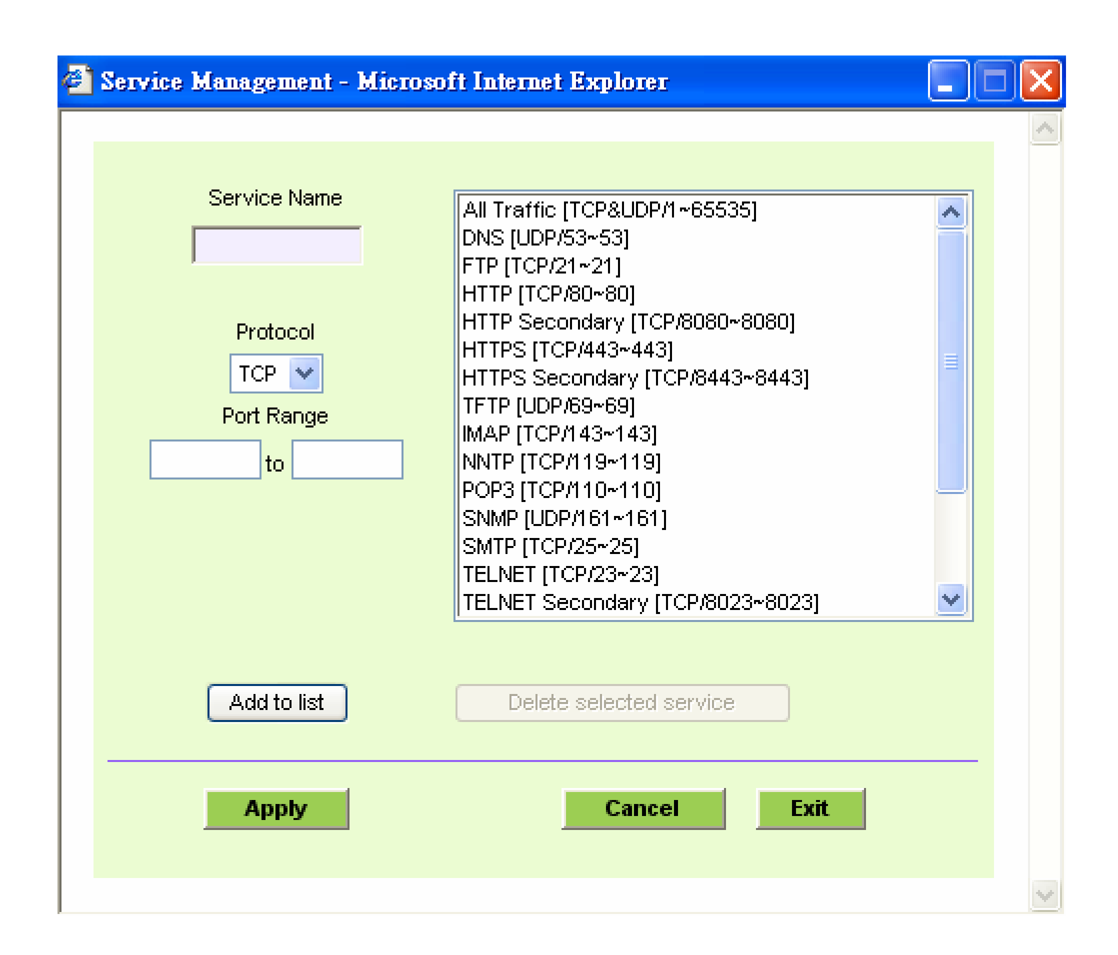
Service Management:

Services Name:	在此自訂選擇欲開啟的服務埠號名稱加入列表中,如 Edonky 等
Protocol:	在此填上欲開啟的服務埠號的位置範圍,如 500~500 或是 2300~2310 等.
Port Range:	開啟此服務功能
Add to List:	增加到開啟服務專案內容列表,最多可新增 30 組.
Delete Selected Services:	刪除所選擇的開啟服務專案之一筆內容





Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數..
Cancel:	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效
Exit:	離開此功能設定畫面



Port Triggering

有一些特殊應用軟體其進出 Internet 的埠號(Port Number)為非對稱的,此時您必須使用此功能選項將一些特殊一用程式使用的埠號填入相關設定中,如以上畫面所示.

Application name: 您可以自訂此特殊應用軟體名稱,方便管理使用!

Trigger Port Range: 輸入由 FVR9416 出 Internet 的使用埠口(Port Number)編號.(如 9000~10000)

Incoming Port Range: 輸入由 Internet 進入的使用埠口(Port Number)編號. (如 2004~2005)

Add to List: 增加到開啟服務專案內容列表.

Delete Selected Application: 刪除所選擇的開啟服務專案之一筆內容

Show Tables: 按下此按鈕即會顯示 Table 上的所有設定專案內容參數.

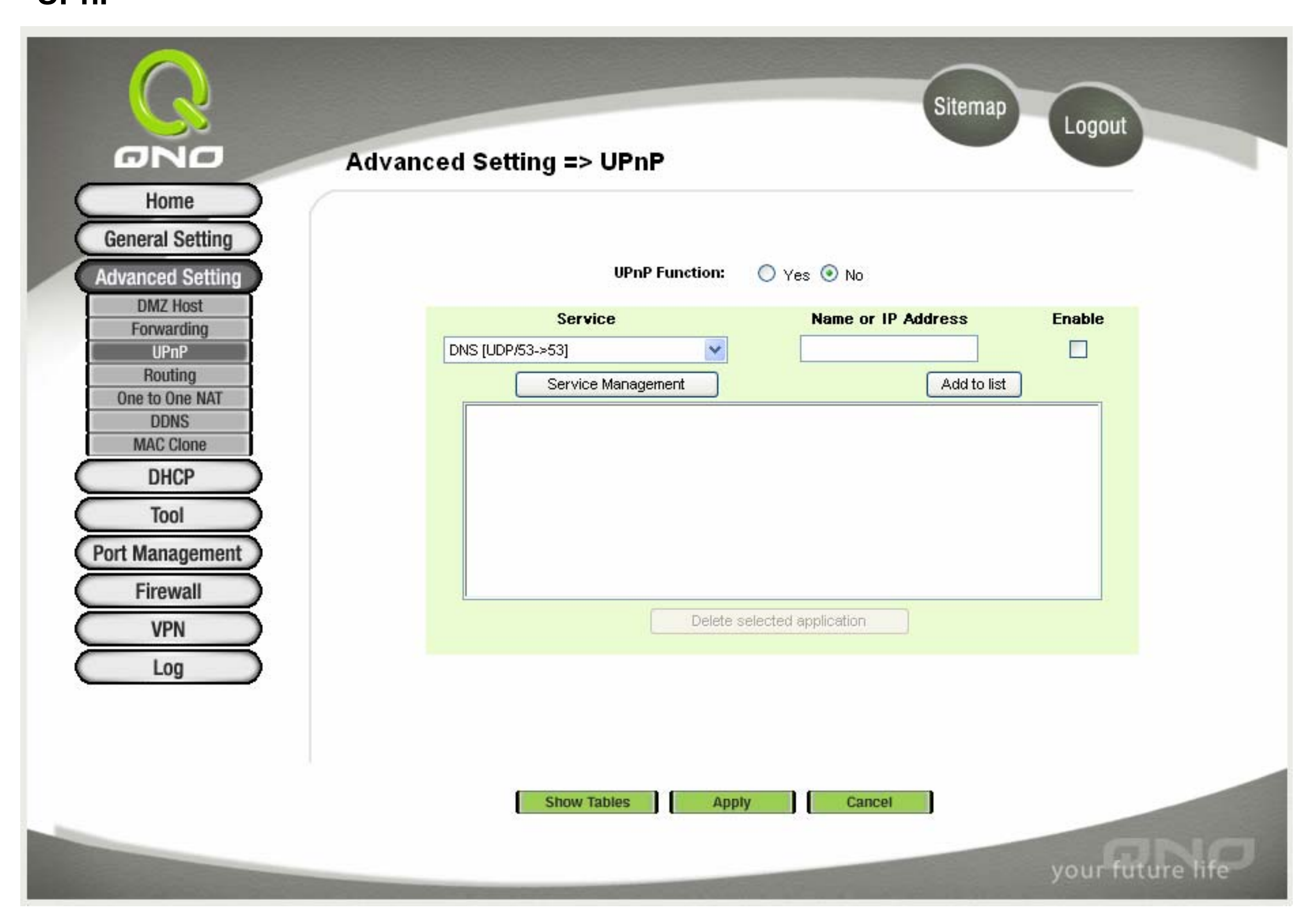
Apply: 按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數..

Cancel 按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

以下為一些常用的埠號需設定到此功能項目中的列表.

Application	Outgoing Control	Incoming Data
Battle.net	6112	6112
DialPad	7175	51200, 51201,51210
ICU II	2019	2000-2038, 2050-2051 2069, 2085,3010-3030
MSN Gaming Zone	47624	2300-2400, 28800-29000

UPnP



UPnP (Universal Plug and Play) 是微軟 Microsoft 所制定的一項通訊協定標準,若是您使用的虛擬主機電腦有支援 UpnP 機制的話(如 WindowsXP),而您也必須相同設定您的電腦使用 UpnP 功能開啟,以便與 FVR9416 路由器協調搭配使用.

Services:	在此選擇欲開啟的 UPnP 的服務號碼預設列表,如 WWW 為 80(80~80), FTP 為 21~21,可參考服務號碼預設列表!.
IP Address:	在此填上 UPnP 相對應的內部虛擬 IP 位置或名稱,如 192.168.1.100
Enable:	開啟此服務功能
Services Management:	新增或刪除管理服務埠號列表
Add to List:	增加到開啟服務專案內容
Delete Selected Services:	刪除所選擇的開啟服務專案之一筆內容
Show Tables:	顯示目前所開啟設定的 UpnP 列表
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數..
Cancel:	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

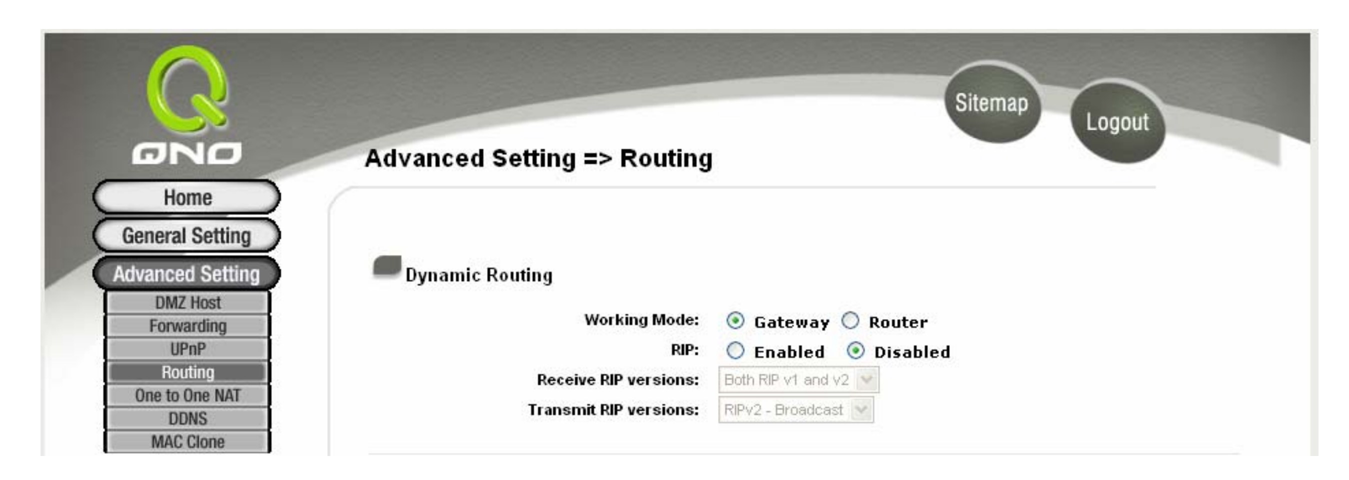


Routing 路由通訊協定

***Dynamic Routing*-動態路由通訊協定**

RIP 是 Routing Information Protocol 的簡稱,在 IP 環境中有 RIP I / RIP II,一般而言網路中大多只有一個路由器,所以決大部份我們會只使用 Static Route(靜態路由通訊),RIP 的使用時機是若存在與網路中有數個路由器,此時不想每台路由器都去定義繞徑表(Routing Table) ,可自動選擇 RIP 通訊協定,且自動將所有路徑更新!

RIP 也是一個很非常簡單的路由協議(Routing Protocol),是採用 Distance Vector 的方式,所謂 Distance Vector 是用以 Router 的個數來作為傳送距離的判斷 , 而不以實際聯機的速率來作判斷,所以在某些時候所選的路徑是經過最少的 Router, 但是並不一定反應速度最快的 Router.



Working Mode: 選擇路由器運作模式為"Gateway"模式(NAT)或是一般路由(LAN to LAN Routing)模式.

RIP: 選擇按鈕"Enable"選擇使用 RIP 動態路由通訊

Transmit RIP Version: 可于上下選擇按鈕選擇使用動態路由通訊 **None, RIPv1, RIPv2, Both RIPv1 and v2** 為傳送動態路由通訊協定的 **"TX"** 功能

Receive RIP Version: 可于上下選擇按鈕選擇使用動態路由通訊 **None, RIPv1, RIPv2-Broadcast, RIPv2-Multicast**, 為接收動態路由通訊協定的 **"RX"** 功能

Show Routing Table: 可使用圖中的功能按紐 "Show Routing Table " 瞭解最新的路徑表

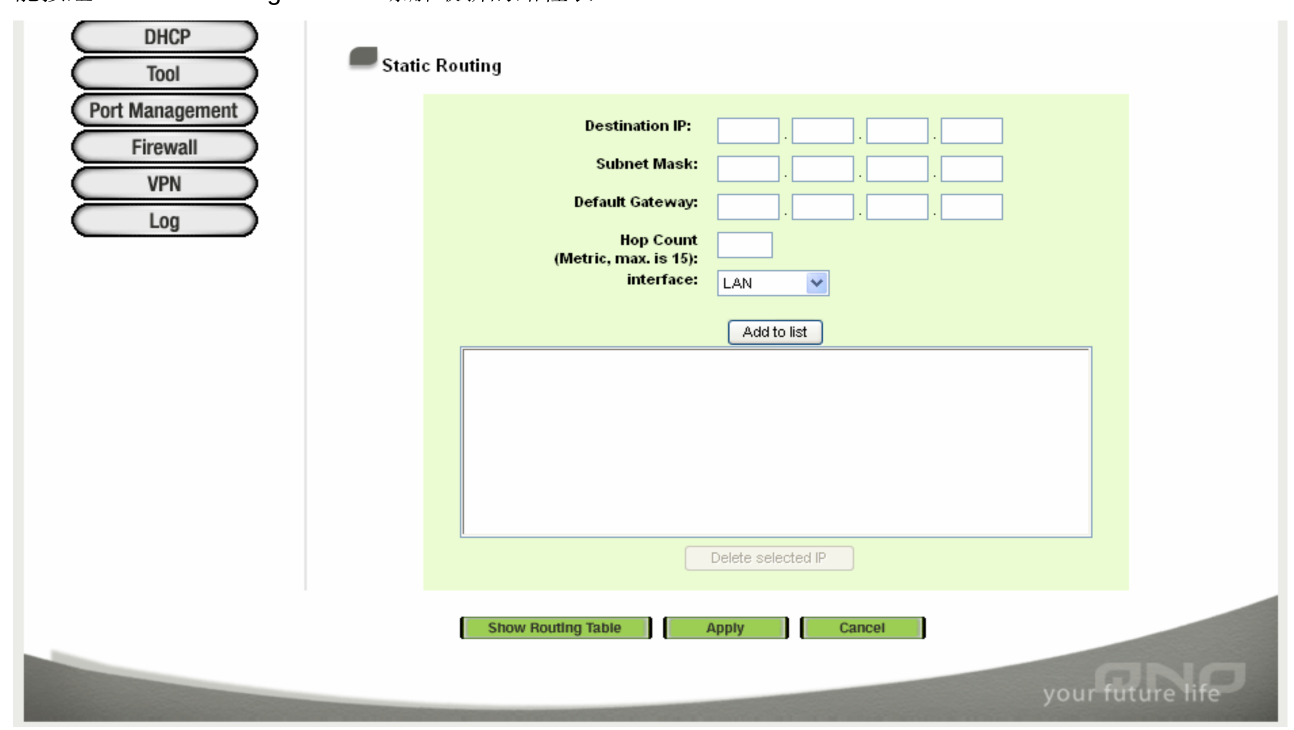
Apply: 按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數.

Cancel: 按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效



Static Routing **靜態路由通訊協定**

如果在您的網路中有多個路由器與 IP 節點子網路,就必需設定 FVR9416 的靜態路由功能(Static Routing),這些功能是讓整個不同的網路節點能自動找尋所需繞徑(Routing)且能讓不同網路節點能相戶存取;可使用圖中的功能按紐 “Show Routing Table “ 瞭解最新的路徑表.



Select Route entry:	可選擇靜態路由表格, FVR9416 共支援了多達 30 組路由表
Delete this entry	刪除一個路由表
Destination IP and **Subnet Mask:**	可填入欲繞徑的遠端網路 IP 節點與子網路節點位置, 如另一個子網路節點為 192.168.2.0/255.255.255.0
Default Gateway:	此網路節點欲繞徑的預設閘道器位置. 如 192.168.2.1
Hop Count:	此節點的路由器層數,如是在 FVR9416 下的二個路由器之一,此應填為 2,預設為 1.(最大為 15)
Interface	此網路節點的連接位置,是位於 WAN 端亦或是 LAN 端.
Delete Selected IP:	刪除一個路徑表
Show Routing Table:	顯示目前最新的路徑表

One-to-One NAT-- 一對一 NAT 對應

當您的寬頻網路為固定制(如 ADSL 固定 8 個 IP 位置)時,因 FVR9416 本身指佔用一個合法 IP 位置,以及 ATU-R 也使用一個合法 IP 位置後,所剩為 4 個合法 IP.欲將此其他的 4 個合法 IP 位置直接對應到 FVR9416 下的 4 個虛擬 IP,可用此功能達成!

使用方法:

當您有使用如“網路遊戲”等任何不支援虛擬 IP 位置的各種應用程式時,可將外部的合法 IP 位置直接對應內部虛擬 IP 位置使用,設定如下填入上方的設定中即可!

範例: 如您有 5 個可用 IP 位置,分別是 210.11.1.1~6,而 210.11.1.1 已經給 FVR9416 的 WAN 合法 IP 使用於一般的 NAT 上,另外還有其他四個合法 IP 可以分別設定到 Multi-DMZ 當中,如下所述

210.11.1.4 → 192.168.1.3

210.11.1.5→ 192.168.1.4

210.11.1.6→ 192.168.1.5

210.11.1.7→ 192.168.1.6

.

Note: FVR9416 廣域網路IP位置(WAN IP -NAT Public) 無法納入此項目的範圍設定中.

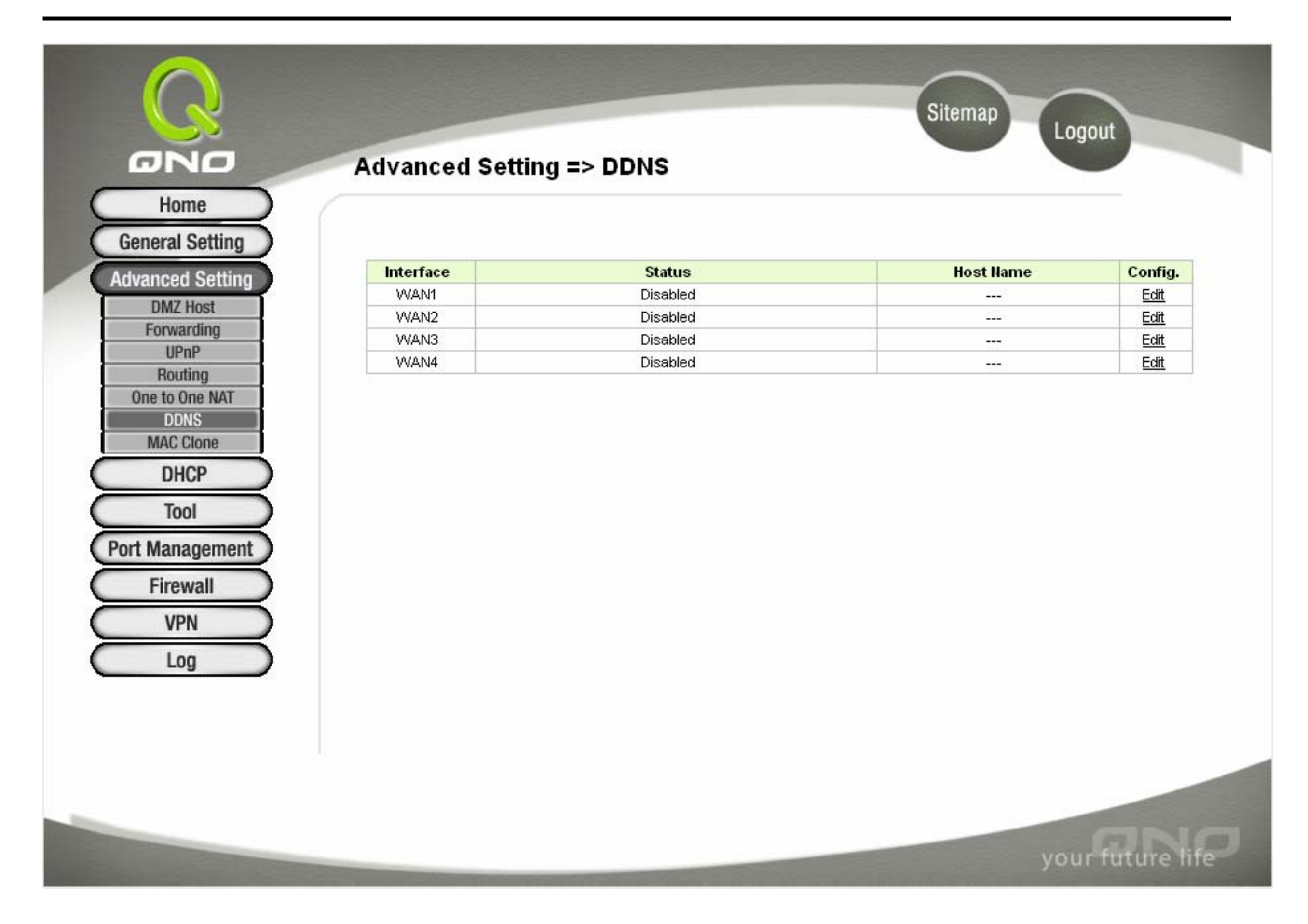
One-to-One NAT: 啟動或關閉一對一 NAT 功能“**Enable**”開啟 **Disable** 關閉 (選擇是否

	開啟此功能)
Private Range Begin:	虛擬 IP 位置起始 IP 位置
Public Range Begin:	外部合法 IP 位置起始 IP
Range Length:	外部合法 IP 位置終止 IP 的數量
Add to List:	加入此設定到一對一 NAT 列表中
Delete selected range:	刪除所選擇的一項一對一 NAT 列表
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數.
Cancel:	按下此按鈕"Undo"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

Note: 一對一的 NAT 模式(One-to-One NAT)將會改變防火牆運作的方式您若設定了此功能, LAN 端所設定的機器或 PC 將會曝露到 Internet 上, 除非到防火牆的 Access Rule 中加入拒絕存取規則專案條件,才可以阻斷由 Internet 進到 LAN 端設定一對一 NAT 的機器或 PC. 您可以按下新增一個一對一 NAT 位置專案(**Add to List)** 按鈕或是選擇刪除一個一對一 NAT 位置(**Delete selected range)**.

DDNS 動態網功能變數名稱稱

"DDNS"目前支持 Dyndns.org 與 3322.org 的動態網址轉換功能,其目的是為了讓使用動態 IP 位置架站或是遠端監控為目的,如 ADSL PPPoE 計時制或是 Cable Modem 的使用者的合法 IP 位置都會隨時間而改變,當此使用者欲架設網站之類的服務,但是因 IP 會隨時變動, 所以本設備提供了動態網址轉換功能,此服務可向 www.dyndns.org 或是 www.3322.org 提出申請,是完全免費的!!



Interface	Status	Host Name	Config.
WAN1	Disabled	---	Edit
WAN2	Disabled	---	Edit
WAN3	Disabled	---	Edit
WAN4	Disabled	---	Edit

請在設定欄(Config.) 的編輯(Edit) 按下該超連結直接進入該設定項目中.

Interface:	使用者所選取的網際網路埠口
DDNS Service:	DDNS 動態網址轉換功能可以選擇“**Disable** 關閉,DDNS.org 與 3322.org 等三項
Username:	使用者名稱:向 DDNS 所設定的名稱
Password:	使用者密碼:向 DDNS 所設定的密碼
Host Name:	動態網址名稱:向 DDNS 所註冊的網址,如 abc.dyndns.org
Internet IP Address	目前所取得的 ISP 之動態合法 IP 位置
Status:	目前 DDNS 的狀態:顯示目前的 DDNS 所更新 IP 功能狀態
Back:	按下此按鈕”Back”即會回上一頁設定畫面
Apply:	按下此按鈕”Apply”即會儲存剛才所變動的修改設定內容參數.
Cancel:	按下此按鈕”Cancel”即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

MAC Clone 變換實體 MAC 位置

此多為使用於雙向 Cable Modem 的用戶,若有發生類似鎖網卡的情況下,可使用此功能將原有網路卡實體層位置(MAC Address:00-xx-xx-xx-xx-xx)填入此專案中以解除鎖定問題!.

Advanced Setting => MAC Clone

Interface	MAC Address	Config.
WAN1	00-07-40-ca-0b-66	Edit
WAN2	00-0c-41-00-00-02	Edit
WAN3	00-0c-41-00-00-03	Edit
WAN4	00-0c-41-00-00-04	Edit

請在設定欄(Config.) 的編輯(Edit) 按下該超連結直接進入該設定項目中.



Advanced Setting => MAC Clone

Home
General Setting
Advanced Setting
DMZ Host
Forwarding
UPnP
Routing
One to One NAT
DDNS
MAC Clone
DHCP
Tool
Port Management
Firewall
VPN
Log

Sitemap
Logout

Interface : WAN1

User Defined WAN MAC Address: 00 - 07 - 40 - ca - 0b - 66

(Default: 00-0c-41-00-00-01)

MAC Address from this PC: 00-0e-a6-6b-70-d9

Back Apply Cancel

Interface:	使用者所選取的網際網路埠口
User Defined WAN1 MAC Address:	目前設備出廠預設的 MAC 位置.
MAC Address From this PC:	目前連接此 PC 的 MAC 位置.
Back:	按下此按鈕"Back"即會回上一頁設定畫面
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數.
Cancel:	按下此按鈕"Undo"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

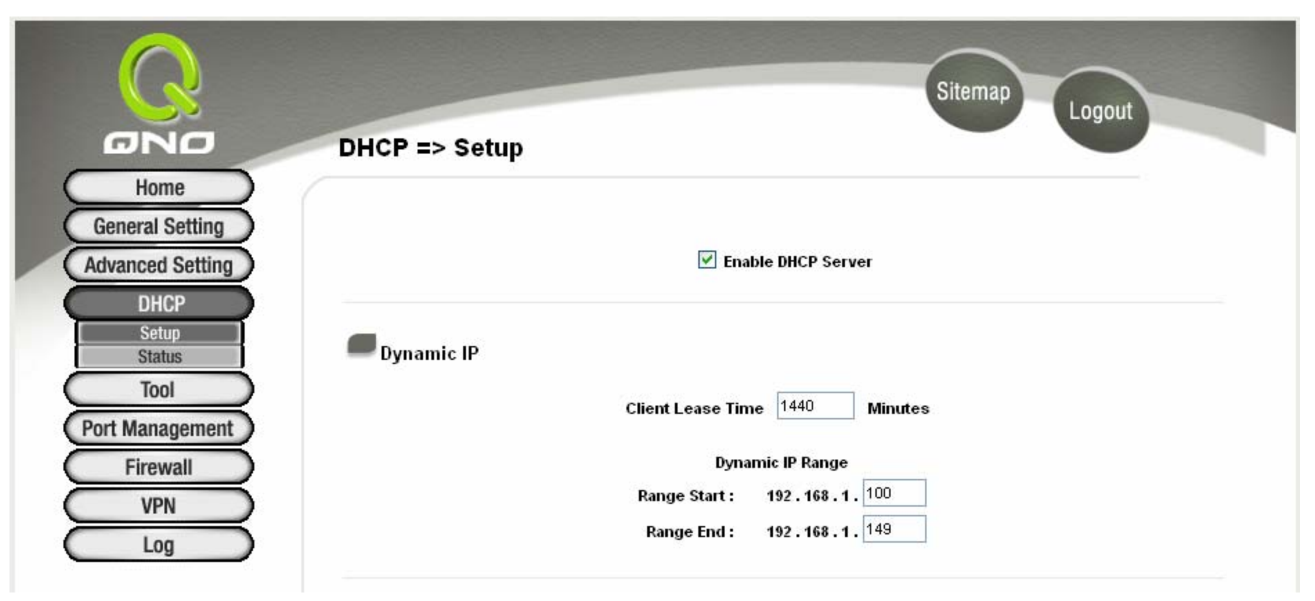
DHCP 發放 IP 伺服器

Setup 設定

因 FVR9416 本身就含有 DHCP 伺服器，所以可以提供區域網路內的電腦自動取得 IP 的功能，(如同 NT 伺服器中的 DHCP 服務，好處是每台 PC 不用去記錄與設定其 IP 位置，當電腦開機後，就可從 FVR9416 自動取得，管理方便。.



Enable DHCP Server: 可選擇開啟 DHCP 伺服器自動派發 IP 位置功能; 若為 Enable 選項, 則所有 PC 都可使用自動取得 IP 位置，反之則無；每台 PC 必需去指定固定虛擬 IP 位置.



***Dynamic IP* 動態 IP**

Client Lease Time: 此設定為發給 PC 端 IP 位置的租約時間,預設為 14400(代表時間為一天),您可以依照實際需求來設定,以分鐘為單位.

Range Start: 此 IP 位置是 DHCP Server 自動派送 IP，意指是從多少 IP 位址開始派送。系統預設為從 100 的 IP 位置開始發放.

Range End: 意指是從多少 IP 地址截止派送。系統預設為從 149 的 IP 位置開始停止發放 IP，原廠設定值可供 50 台電腦自動取得 IP 位址,您可以是實際情況增減使用!

***Static IP* 靜態 IP**

Static IP address 輸入 PC 端固定虛擬 IP 位置

MAC: 輸入 PC 端固定實體 MAC 位置

Add to List: 加入此設定到 Static IP 列表中

Delete selected Entry: 刪除所選擇的 Static IP 列表

Static IP

Static Entry

Static IP Address:

MAC Address:

Add to list

Delete selected Entry

DNS

DNS Server (Required) 1: 0 . 0 . 0 . 0

2: 0 . 0 . 0 . 0

WINS

WINS Server : 0 . 0 . 0 . 0

Apply Cancel

DNS Server

此設定為發給 PC 端 IP 位置的 DNS 網域伺服器查詢位置,您可以直接輸入此伺服器的 IP 位置.

DNS Server (Required)1	輸入 DNS 網域伺服器的 IP 位置.預設值為 0.
2	輸入 DNS 網域伺服器的 IP 位置.預設值為 0.

WINS

若您的網路上有解析如 Windows 的電腦名稱伺服器的話,您可以直接輸入此伺服器的 IP 位置

.

WIN Server:	輸入 WIN 網域伺服器的 IP 位置.預設值為 0.
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數.
Cancel:	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

Status 狀態顯示

DHCP => Status

Status

DHCP Server : 192.168.1.1
Dynamic IP Used : 0
Static IP Used : 0
DHCP Available : 50
Total : 50

Client Table

Client Host Name	IP Address	MAC Address	Leased Time	Delete

Refresh

此狀態表為顯示 DHCP 伺服器的目前使用狀態與設定紀錄等,以便提供管理人員需要時做網路設定參考資料.以下針對其內容做介紹:

DHCP Server:	目前 DHCP 伺服器的 IP 位置
Dynamic IP Used:	目前 DHCP 伺服器已經發放動態 IP 的數量
Static IP Used:	目前 DHCP 伺服器已經發放固定 IP 的數量
DHCP Available:	目前 DHCP 伺服器可以發放的 IP 數量
Total:	目前 DHCP 伺服器所設定可發放的 IP 總數量
Client Host Name:	目前此台電腦的電腦名稱
IP Address:	目前此台電腦所取得的 IP 位置
MAC Address:	目前此台電腦的 MAC 網路實體位置
Leased Time:	DHCP 目前核發 IP 位置的租約時間

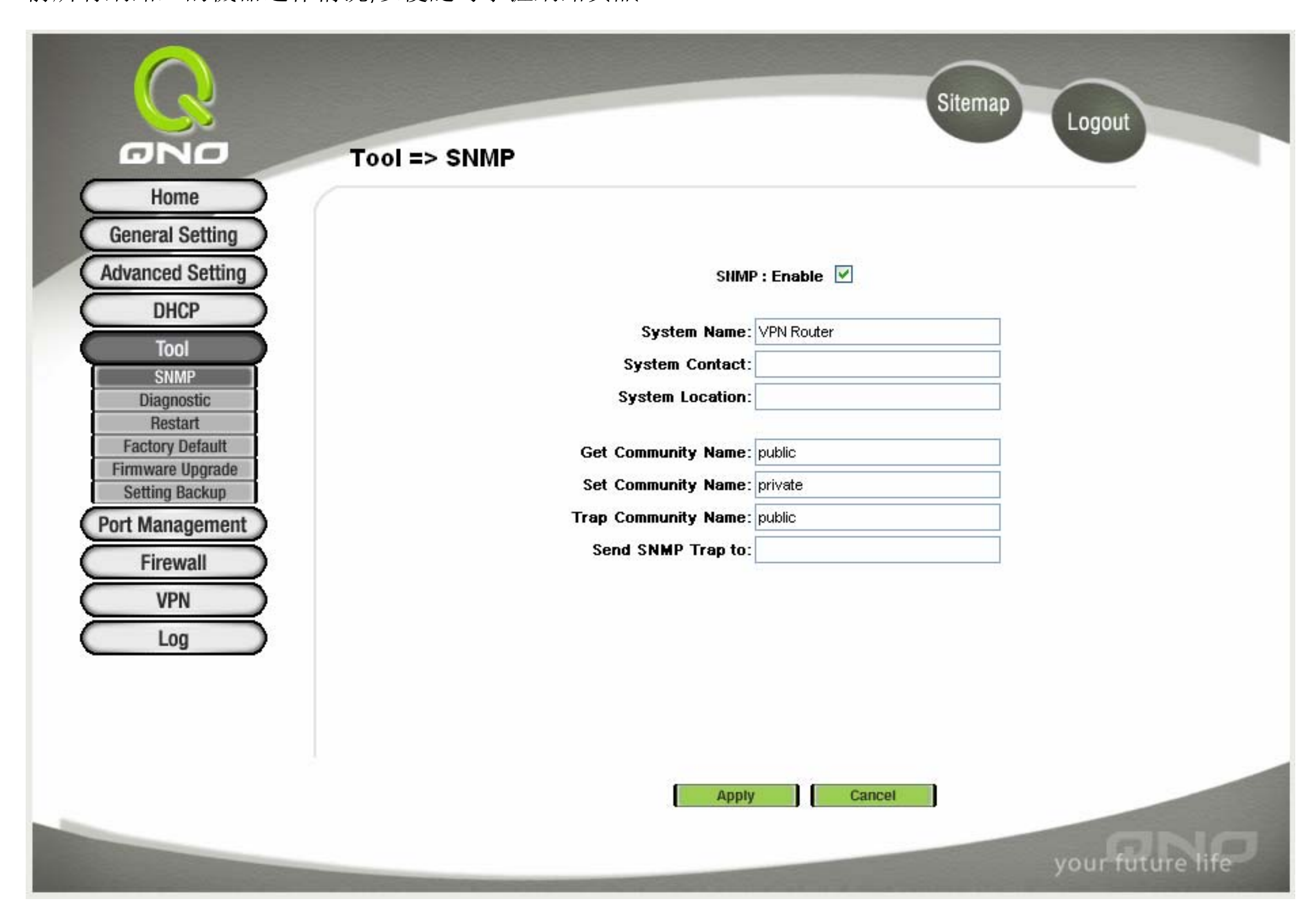


Delete:	刪除此筆核發 IP 紀錄

Tool 工具程式

SNMP 網路通訊

SNMP 為 Simple Network Management Protocol 的縮寫,意指網路管理通訊協定,此為網路上重要的管理專案依據之一,透過此 SNMP 通訊協定,可以讓已經具備有網路管理的程式(如 SNMP Tools-HP Open View)等網管程式做即時管理之通訊使用, FVR9416 支援標準 SNMP v1/v2c,可以搭配標準 SNMP 網路管理軟體來得知目前所有網路上的機器運作情況,以便隨時掌握網路資訊.



Enable SNMP:	將 SNMP 功能開啟,系統預設為開啟此功能.
System Name:	設定機器的名稱,如 FVR9416
System Contact:	設定機器的管理聯繫人員名稱,如 John
System Location:	設定機器的目前所在位置,如 Taipei

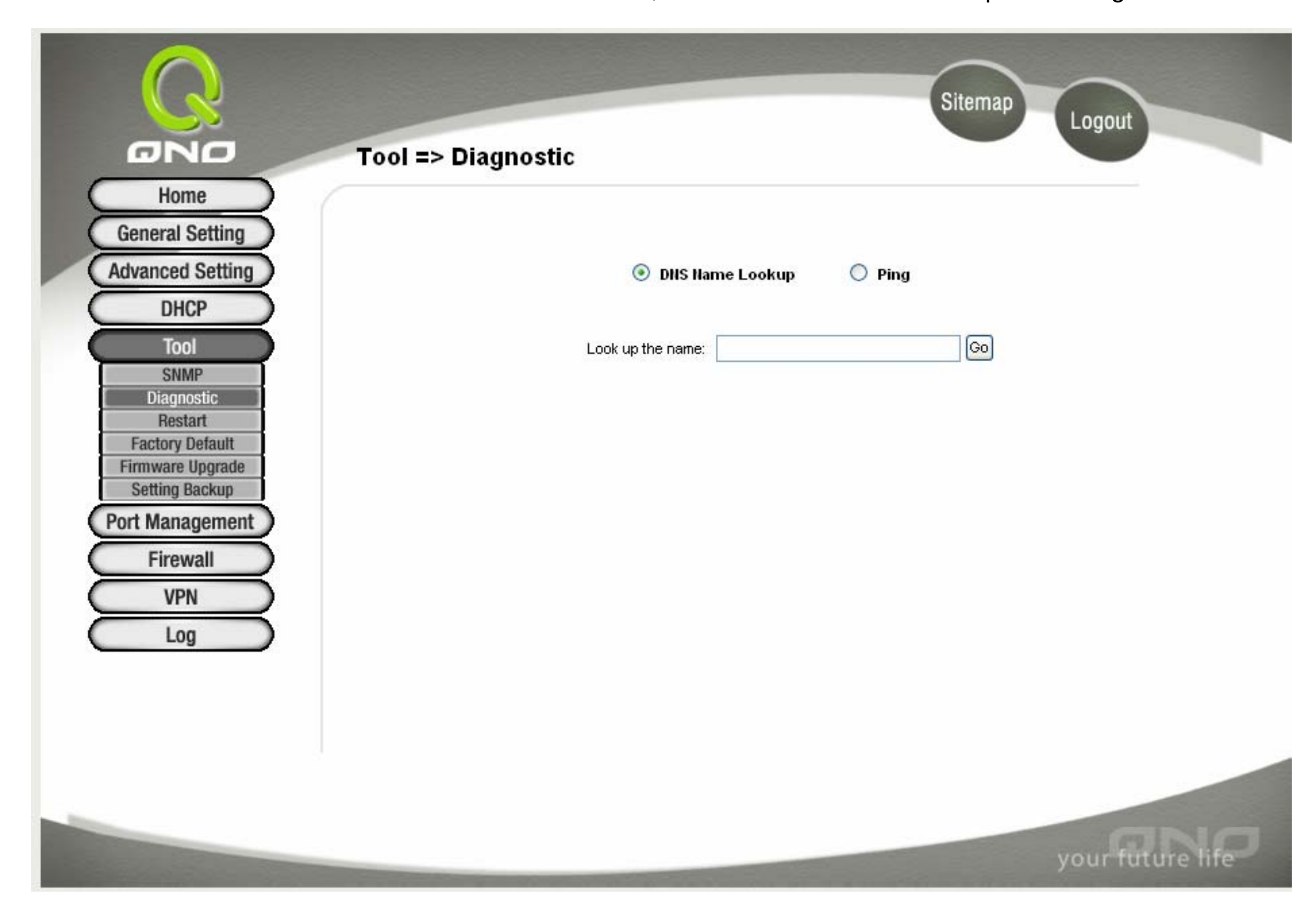




Get Community Name:	設定一組管理者參數可以取得此機器的專案資訊,系統預設"Public"
Set Community Name:	設定一組管理者參數可以設定此機器的專案資訊,系統預設"Private"
Trap Community Name:	設定一組管理者參數可以傳送 Trap 的資訊
Send SNMP Trap to:	設定一組 IP 位置或是 Domain Name 名稱的接收 Trap 訊號主機
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數.
Delete:	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

Diagnostic 線上聯機除錯測試

FVR9416 提供簡易的線上測試機制方便于除錯時使用,此除錯機制包含 DNS Lookup 以及 Ping 二種.



DNS Name Lookup網功能變數名稱稱查詢測試

請於此測試畫面輸入您想查詢的網域主機位置名稱,如www.abc.com 然後按下Go的按鈕開始測試,測試結果會顯示於此畫面上.

Ping封包傳送/接收測試

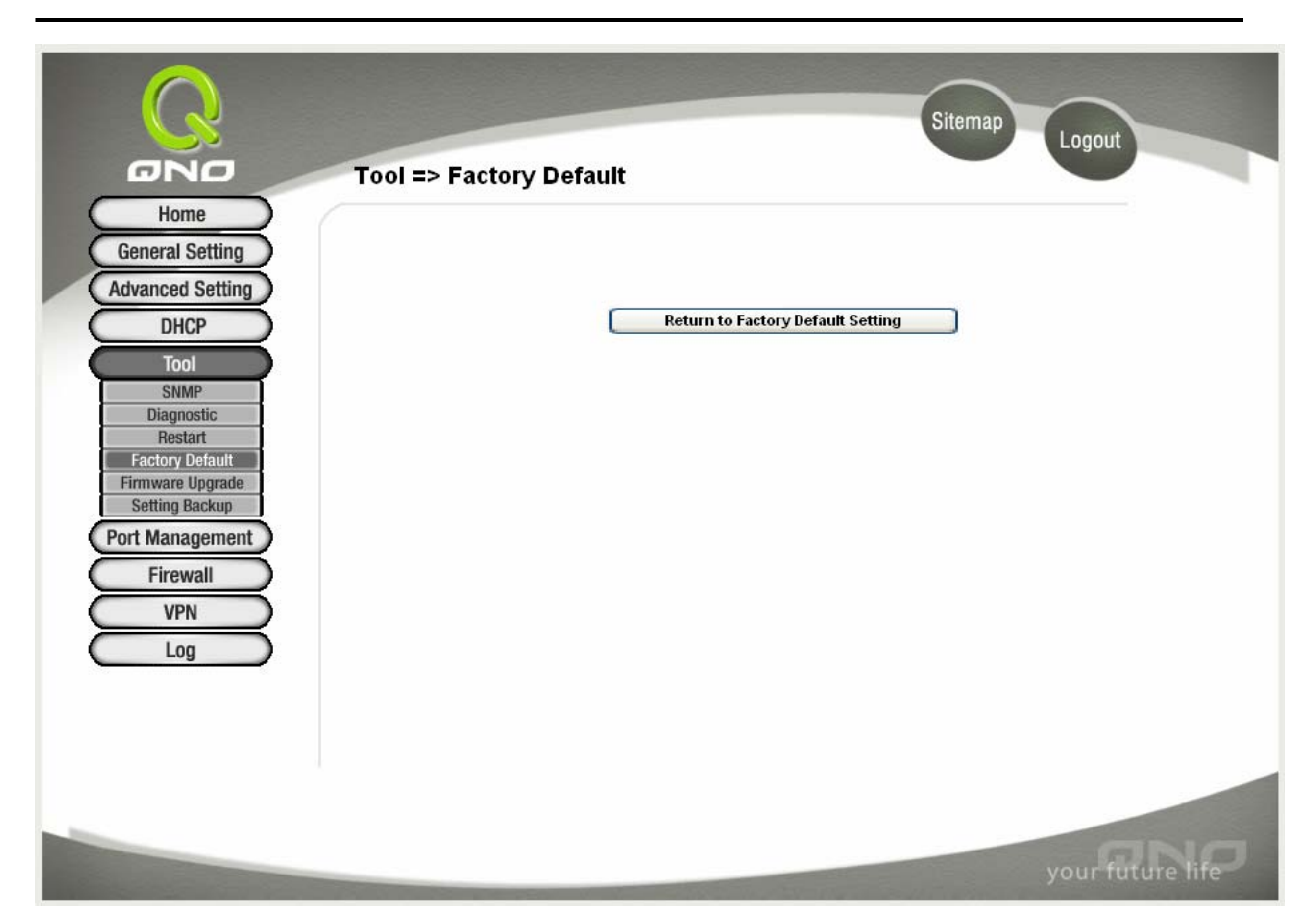
此專案為主要提供管理者瞭解對外聯機的實際狀況,可以藉由此功能瞭解網路上的電腦是否存在!

請於此測試畫面輸入您想測試的主機位置 IP,如 192.168.5.20 按下 Go 的按鈕開始測試,測試結果會顯示於此畫面上..

Restart 重新啟動

您可以於此工具中選擇 FVR9416 系統重新開機功能,請按下 **Restart Router** 按鈕即可重新開機啟動.

Factory Default-回復原出廠預設值



若是選擇**"Return Factory Default Setting"**, FVR9416 會將所有的 FVR9416 上面的設定清除,並重新開機; 除非有必要,否則使用此功能會將機器所有的資料清除!

.

Firmware Upgrade 系統韌體升級

Sitemap Logout

Tool => Firmware Upgrade

Home
General Setting
Advanced Setting
DHCP
Tool
SNMP
Diagnostic
Restart
Factory Default
Firmware Upgrade
Setting Backup
Port Management
Firewall
VPN
Log

瀏覽...

Firmware Upgrade Right Now

Warning: 1. When choosing previous firmware versions, all settings will restore back to default value.
2. Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button.
3. Please don't close the window or disconnect the link, during the upgrade process.

your future life

Firmware Upgrade

此設定可以於 FVR9416 的 Web 設定畫面中直接升級韌體的功能,並請您於升級前先確認韌體版本資訊,選擇流覽至韌體-Firmware 存放資料夾選擇該檔案後,按下 **Firmware Upgrade Right Now** 做升級.

.

Setting Backup 系統設定參數儲存

Tool => Setting Backup

Import configuration File

Import

Export configuration File

Export

Import Configuration File:

此功能為將之前所儲存的設定參數的內容回存到機器中! 並請您於升級前先確認韌體版本資訊,選擇流覽至備份參數檔案-"config.exp"存放資料夾選擇該檔案後,按下 **Import** 按鈕做設定檔案匯入.

Export Configuration File:

此功能為儲存備份 FVR9416 的設定參數,! 按下 **Export** 按鈕,選擇至備份參數檔案-"config.exp"存放資料夾位置,按下儲存即可.



Port Management 網路實體埠口管理

于 FVR9416 防火牆路由器中,使用管理者可以設定 WAN 埠口的數目與網路實體聯機於每一個乙太網路埠口,如連接速率(Speed),工作模式(Half &Full),高低優先權(Priority)或是自動偵測(Auto-negotiation)等乙太網路埠口的功能.

Port Setup 網路埠口設定

Home
General Setting
Advanced Setting
DHCP
Tool
Port Management
Port Setup
Port Status
Firewall
VPN
Log

Sitemap Logout

Port Management => Port Setup

Please choose how many WAN ports you prefer to use : 4 (Default value is 4)

Port ID	Interface	Disable	Priority	Speed	Duplex	Auto Negotiation
1	LAN	☐	Normal	10M 100M	Half Full	☑ Enable
2	LAN	☐	Normal	10M 100M	Half Full	☑ Enable
3	LAN	☐	Normal	10M 100M	Half Full	☑ Enable
4	LAN	☐	Normal	10M 100M	Half Full	☑ Enable
5	LAN	☐	Normal	10M 100M	Half Full	☑ Enable
6	LAN	☐	Normal	10M 100M	Half Full	☑ Enable
7	LAN	☐	Normal	10M 100M	Half Full	☑ Enable
8	LAN	☐	Normal	10M 100M	Half Full	☑ Enable
9	LAN	☐	Normal	10M 100M	Half Full	☑ Enable
10	LAN	☐	Normal	10M 100M	Half Full	☐ Enable
11	LAN	☐	Normal	10M 100M	Half Full	☑ Enable
12	WAN4	☐	Normal	10M 100M	Half Full	☑ Enable
13	WAN3	☐	Normal	10M 100M	Half Full	☑ Enable
14	WAN2	☐	Normal	10M 100M	Half Full	☑ Enable
15	WAN1	☐	Normal	10M 100M	Half Full	☑ Enable
DMZ	DMZ	☐	Normal	10M 100M	Half Full	☑ Enable

Apply Cancel

your future life

Basic Per Port Config. 乙太網路埠口設定

Port ID: 於此顯示每個埠的編號

Port Disable: 此為設定乙太網路的埠口開啟或是關閉的功能,若是打勾的話,則此乙太網路埠口立即被關閉無法連接使用.預設為開啟無打勾

Priority: 此為設定此乙太網路的埠口封包傳送高低優先權設定,若是此 Port 設定為 High 的話,則最優先使用傳送封包的權利,預設值為-Normal 優



	先順序為一般
Speed:	此為設定此乙太網路的埠口網路實體連接速率選項,您可以設定為 10Mbps 或是 100Mbps 連接速度.
Duplex:	此為設定此乙太網路的埠口網路實體連接速率工作模式選項,您可以設定為 Half –半雙工模式或是 Full-全雙工模式運作.
Auto-negotiation:	此為設定此乙太網路的埠口網路實體連接速率自動偵測模式,若是勾選的話,自動偵測所有連接埠口的信號與調整.

按下 Apply 按鈕可以儲存設定或是按下 Cancel 按鈕可以取消設定更改

Port Status 網路埠口狀態即時顯示

使用管理者可以於此專案中,選擇所需要監看的乙太網路埠口各項即時參數顯示,如下圖.

Sitemap Logout

Home
General Setting
Advanced Setting
DHCP
Tool
Port Management
Port Setup
Port Status
Firewall
VPN
Log

Port Management => Port Status

Port ID : 1

Summary

Type	10Base-T / 100Base-TX
Interface	LAN
Link Status	Down
Port Activity	Port Enabled
Priority	Normal
Speed Status	10 Mbps
Duplex Status	Half
Auto negotiation	Enabled

Statistics

Port Receive Packet Count	164453
Port Receive Packet Byte Count	35108106
Port Transmit Packet Count	237216
Port Transmit Packet Byte Count	249909015
Port Packet Error Count	0

Refresh

your future life

於網路埠口狀態-Port Status 整體資訊**(Summary)** 表格專案中, 此部份會顯示目前埠口硬體設定專案如網路連接型態(Type), 線路聯機狀態(Link Status), 埠口使用狀態(Port Activity 開-on 或關-off), 埠口優先權設定(Priority- (高-High 或一般-Normal), 網路連接速率(Speed Status-10Mbps 或 100Mbps), 雙工模式(Duplex Status-半雙工 half 或全雙工-full),自動偵測模式(Auto negotiation(啟動 Enabled 或關閉 Disabled).

于網路埠口實時顯示**(statistics)** 資訊表格專案中，將會顯示目前此埠口的封包重送資料,包含傳送/接收封包計算(receive/transmit packet count)/以及封包傳送/接收 Byte 數計算(packet byte count)與 錯誤封包統計(Port Packet Error Count) 等. 您可以按下 **Refresh** 按鈕重新整理所有的即時資訊顯示.

Firewall 防火牆設定

General 一般

從防火牆功能選項當中(Firewall->General), 管理者可以設定 FVR9416 防火牆路由器關閉(deny)或是允許(allow)任何的封包進出 Internet . 您可以選擇設定不同的封包過濾於不同的使用者存取規則條件從內部到外部(Inside-LAN to Outside-WAN),或是設定以 IP 位置以及通訊埠口號碼(Port Number)不同的封包過濾於 Internet 存取規則條件從外部到內部(Outside-WAN to Inside-LAN).

Firewall: 此為設定 FVR9416 的管理密碼,請選擇更改密碼 **"Password Change"** 填入您的新密碼,然後在**"Password Confirm"**再填寫確認一次,以便更改 FVR9416 的管理密碼,在此建議您務必更動原有



	admin 的預設密碼較為安全
SPI(Stateful Packet Inspection):	此為封包主動偵測檢驗技術(Stateful Packet Inspection),防火牆主要運作在網路的層級，但是藉由執行對每個連結的動態檢驗，也擁有應用程式的警示功能，讓封包檢驗型防火牆可以拒絕非標準的通訊協定所使用的連結.
DoS(Denial of Service):	此為保護 DoS 攻擊,如 SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing 等.
Block WAN Request:	若是選擇 **Enable** 的話,則 FVR9416 會關閉對外的 ICMP 與不正常聯機的封包回應,預設值為開啟.(若您是使用 Cable 聯機的話,此選項請開啟)
Remote Management:	遠端管理功能,若您要透過 Internet 直接聯機進入路由器的設定畫面,必需將此功能開啟,並于遠端使用 IE 於網址填入 FVR9416 的外部合法 IP 位置(WAN Port IP),並加上預設可修改的控制埠口(預設為 80,可更改),如 http://210.11.11.1 才可進入設定畫面!!
Multicast Pass Through:	網路上有許多影音串流媒體,使用廣播方式可以讓您的 Client 端接收此類封包訊息格式.
MTU(Maximum Transmission Unit):	MTU 為 Maximum Transmission Unit 的縮寫，一般預設的 default 為 1,500. 但是在不同的網路環境中，應該是有不同的數值. 尤以 ADSL PPPoE 的狀況為最多(ADSL PPPoE MTU Size:1492); 不過許多的 Server 與 ADSL PPPoE 用戶的 MTU Size 相關,一般預設即可,不需做任何調整

Access Rules 網路存取規則

網路存取規則依照 IP address(IP 位置), Destination IP address(目地端 IP 位置), 與 IP protocol type(IP 通訊協定型態) 來管理所有的網路封包流量是否可以通過 FVR9416 防火牆的存取.

FVR9416 擁有簡而易懂的網路存取規則條例工具. 管理者可自訂的網路存取規則條例，可以選擇關閉或是開啟並保護所有對網際網路 Internet 的存取.以下就針對 FVR9416 的網路存取規則條例做一說明:

以下為 FVR9416 預設的網路存取規則條例:

* All traffic from the LAN to the WAN is allowed-從 LAN 端到 WAN 端的封包預設為可以通過
* All traffic from the WAN to the LAN is denied.- 從 WAN 端到 LAN 端的封包預設為關閉
* All traffic from the LAN to the DMZ is allowed.- 從 LAN 端到 DMZ 端的封包預設為可以通過
* All traffic from the DMZ to the LAN is denied-從 DMZ 端到 LAN 端的封包預設為關閉.
* All traffic from the WAN to the DMZ is allowed-從 WAN 端到 DMZ 端的封包預設為開啟.
* All traffic from the DMZ to the WAN is allowed-從 DMZ 端到 WAN 端的封包預設為開啟.

使用者可以自定存取規則並且超越 FVR9416 的預設存取條件規則，但是以下的四種額外服務專案為永遠開啟,不受其他自訂規則所影響:

* HTTP 的服務從 LAN 端到 FVR9416 預設為開啟的.(為了管理 FVR9416 使用)
* DHCP 的服務從 LAN 端到 FVR9416 預設為開啟的. (為了從 FVR9416 自動取得 IP 位置使用)
* DNS 的服務從 LAN 端到 FVR9416 預設為開啟的. (為了解析 DNS 服務使用)
* Ping 的服務從 LAN 端到 FVR9416 預設為開啟的.(為了連通測試 FVR9416 使用)

Sitemap Logout

Home
General Setting
Advanced Setting
DHCP
Tool
Port Management
Firewall
General
Acess Rule
Content Filter
VPN
Log

Firewall => Access Rule

Jump to 1 /1 page   5 entries per page

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day		Delete
	☑	Allow	All Traffic [0]	LAN	Any	Any	Always			
	☑	Deny	All Traffic [0]	WAN1	Any	Any	Always			
	☑	Deny	All Traffic [0]	WAN2	Any	Any	Always			

Add New Rule   Restore to Default Rules

your future life

除了預設規則以外，所有的網路存取規則都會顯示於此規則列表中,您可以依照或是自己選擇高低優先權 **(Priority)** 於每一個網路存取規則專案中. 按下 Edit 按鈕可以設定網路存取規則專案，以及按下 Trash Can icon 可以刪除網路存取規則專案.

按下 **Add New Rule** 新增新的網路存取規則按鈕可以新增一項新的存取規則，或是按下 **Restore to Default Rules** 可以回復原有預設存取規則專案，以及刪除所有的自訂規則內容回到出廠預設存取規則.

Add a new Rule 增加新的管制規則

Services: 使用者可以自訂網路使用流量的來源端 IP 位址,目的端 IP 位址以及 IP 通訊協定等可以經由防火牆控管

Action: 此為設定 FVR9416 的管制條例動作:
Allow:允許此管制條例通過
Deny:關閉此管制條例

Service: 選擇服務專案內容,可以上下做選單的選擇.

Service Management: 若是您想要管制的服務內容沒有存在於預設列表內的話,您可以按下右方的 **Service Management** –服務管理 新增一個服務內容,輸入一個服務名稱-Service Name 以及通訊協定與埠口- Protocol & Port ,以及按下 Add-新增按鈕即可新增一個管制服務專案內容.

Log: 使用者可以選擇是否要將此管制條例存入 Log.若是符合此件的話,將此 Log 存入或是不需要 Log 的資訊

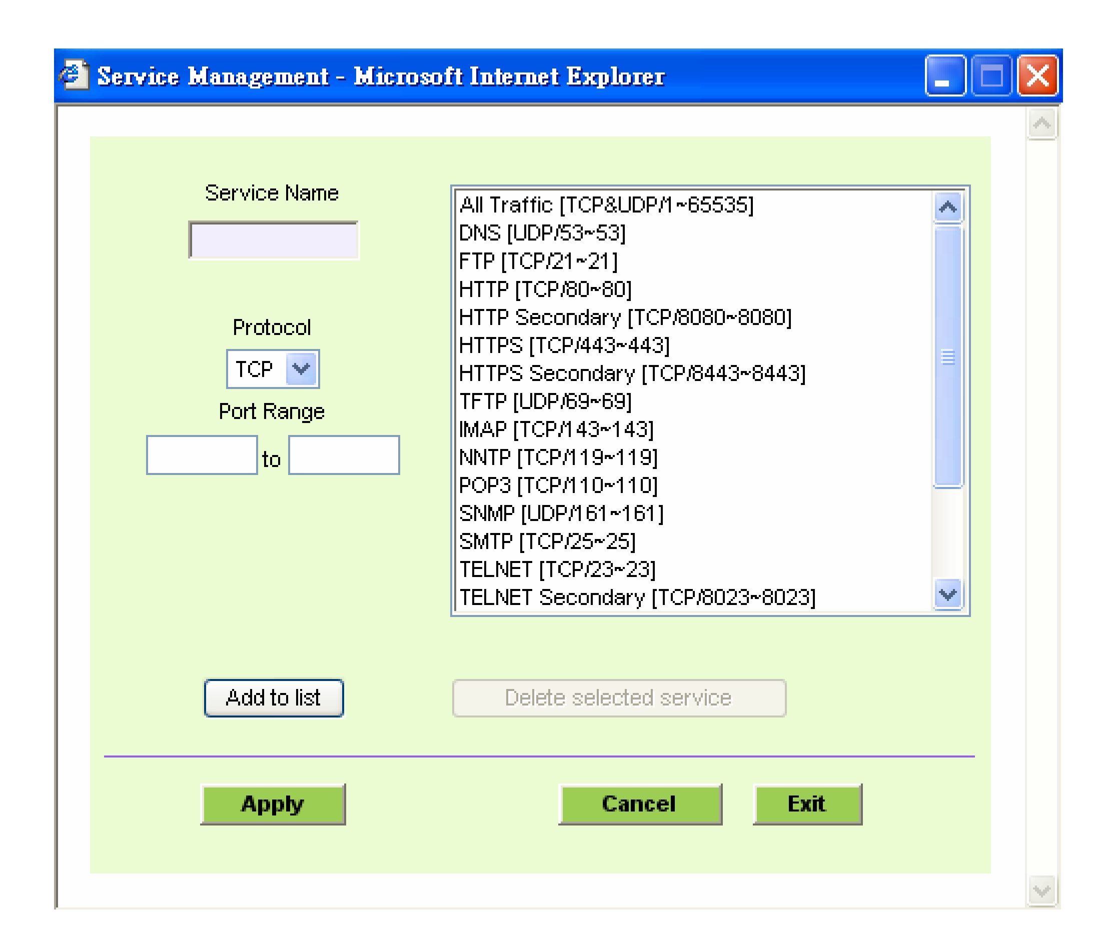
Source Interface: 選擇來源的封包位置介面(如 LAN, WAN1~WAN4, Any)專案內容,可以上下做選單的選擇.

Source IP: 選擇來源封包的 IP 位置(如 **Any**, **Single** or **Range**),若是選擇 Single 或是 Range 的話,請輸入此單一或是一區段範圍的 IP 位置.

Destination IP: 選擇目的端封包的 IP 位置(如 **Any**, **Single** or **Range**),若是選擇

	Single 或是 Range 的話,請輸入此單一或是一區段範圍的 IP 位置.
Scheduling:	是否需要將此管制條例安排於特定的管制時間設定
Apply this rule (time parameter):	可選擇 Always-都關閉(預設),或是選擇每週幾以及從幾點到幾點做管制

Services Management: 管制服務內容專案管理



Services Name:	新增服務專案內容,可自訂名稱.
Protocol:	新增服務專案通訊協定為 TCP 或是 UDP 封包格式.
Port Range:	設定開啟此服務的埠口位置範圍,如 Port 從 9000~9002.
Add to List:	增加此新增的服務專案內容到服務表列內
Delete Selected Services:	選擇刪除服務專案內容從服務表列內



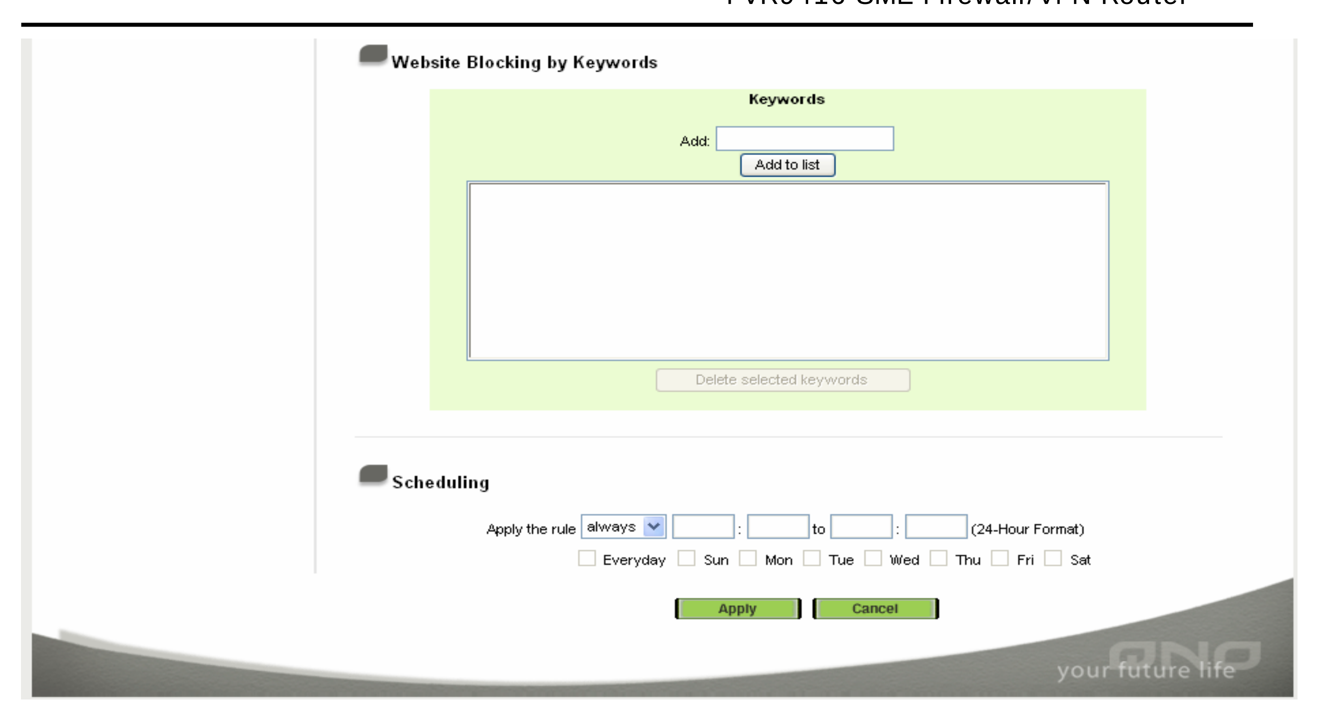
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數.
Cancel:	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效
Exit:	跳出此服務表管理畫面

Content Filter 網頁內容管制



Block Forbidden Domains:	選擇打勾開啟網頁內容管制功能,預設為關閉.
Add:	填寫欲管制的網頁內容,如 www.playboy.com
Add to List:	按下 Add 按鈕新增此一欲管制的網頁內容.
Delete Selected Domain:	可以使用滑鼠點選一個或多個管制的網頁內容,然後按下即可刪除

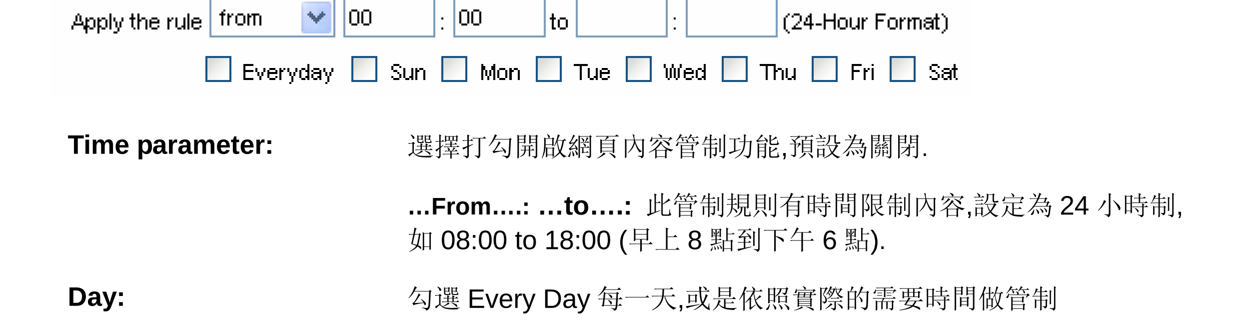




Scheduling

此日期與時間項目功能為管制該條例所生效的實際時間才進行管制,如管制時間為週一到週五,早上八點到下午六點,您可以依照以下說明適當的管制您所需要的時間參數設定.

Apply this rule:



Time parameter: 選擇打勾開啟網頁內容管制功能,預設為關閉.

...From....: ...to....: 此管制規則有時間限制內容,設定為 24 小時制,如 08:00 to 18:00 (早上 8 點到下午 6 點).

Day: 勾選 Every Day 每一天,或是依照實際的需要時間做管制

VPN 虛擬私有網路

Summary 目前所有的 VPN 狀態顯示

此 VPN 狀態可以顯示目前有關 VPN 方面的即時狀態包含通道-Tunnel ,設定參數以及 **GroupVPN-VPN** 群組狀態等資訊.

Summary:



此為顯示目前有多少 VPN 通道已經設定使用,還剩下多少通道可以提供設定, FVR9416 可同時支援共 200 組 VPN 通道(tunnels).

Detail: 按下此 Detail 按鈕可以顯示如以下畫面的目前所有 VPN 組態,讓管理者清楚的管理所有 VPN 連接資訊.



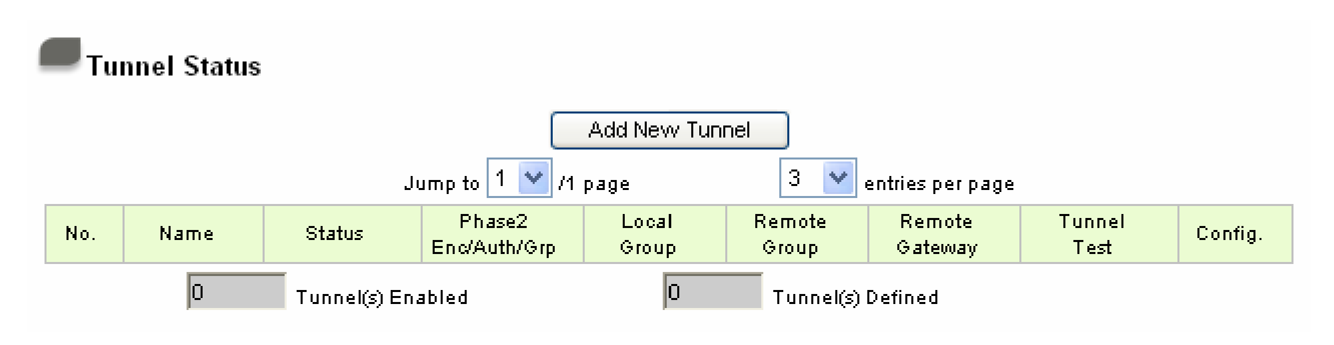
.

WAN1 IP: 192.168.5.140 WAN2 IP: 0.0.0.0 WAN3 IP: 0.0.0.0 WAN4 IP: 0.0.0.0 Wed Sep 1 06:01:03 2004

No.	Name	Status	Phase 2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway

Close

Tunnel Status: VPN 通道目前狀態顯示

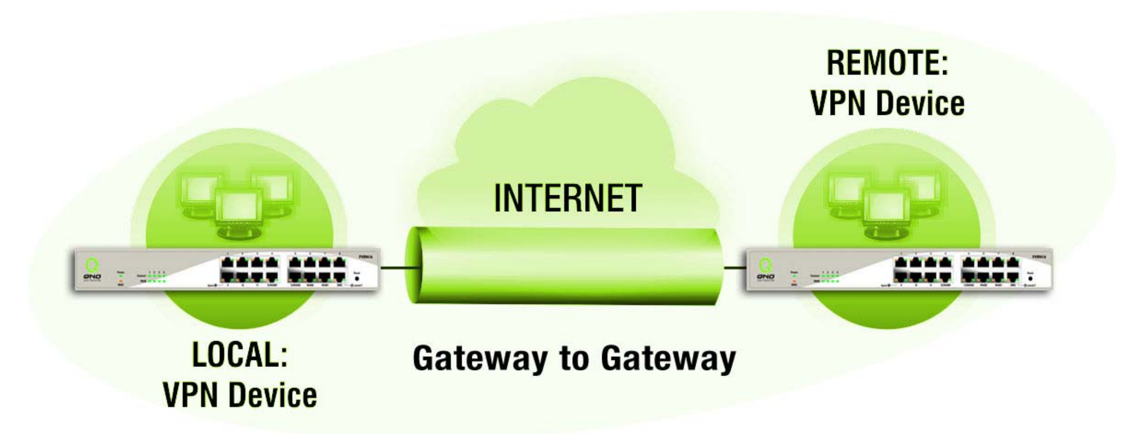


Add New Tunnel: 新增一條新的 VPN 通道設定

FVR9416 可以支援包含 **Gateway to Gateway Tunnel** 或是 **Client to Gateway Tunnel**

Gateway to Gateway:

以下的 VPN 網路連接為運作於 Gateway to Gateway 模式環境,VPN 通道連接為 2 台 VPN 路由器分別透過網際網路 Internet 所組成,當您按下新增"Add Now" 的話, 將會直接導引到 **Gateway to Gateway** 的設定頁面上..

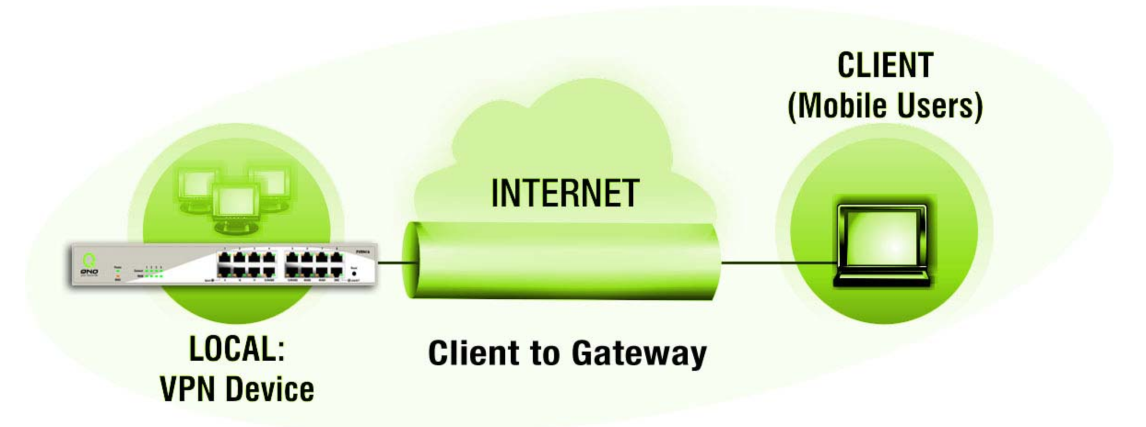


Client to Gateway:

以下的 VPN 網路連接為運作於 Client to Gateway 模式環境,VPN 通道連接為一台 PC 以及一台 VPN 路由器分別透過網際網路 Internet 所組成,當您按下新增"Add Now" 的話, 將會直接導引到 **Client to Gateway** 的設



定頁面上.



以下就針對"**Tunnel Status**" VPN 通道目前狀態顯示做完整解說.

Page: Previous page, Next page, Jump to page / pages and entries per page　您可以按下上一頁(Previous page)與下一頁(Next page)按鈕跳到您想監看的 VPN 通道畫面上,或者您可以直接選擇每一次所顯示的頁次,來監看您的所有 VPN 通道狀態,如(3, 5, 10, 20, All)..

Tunnel No:　當您設定 FVR9416 內建之 VPN 功能時,請選擇您要設定的 Tunnel 通道編號,最多可支援 200 條 VPN 通道設定(Gateway To Gateway 或 Client To Gateway.

Status:　于此狀態顯示已經聯機成功-Connected,電腦聯機名稱-Hostname Resolution Failed, Resolving Hostname 以及等待聯機-Waiting for Connection 等資訊,若是管理者選擇手動-Manual 設定 IPSec 通道,則此狀態會顯示手動-Manual 設定與沒有測試此項手動設定功能狀態模式

Name:　目前聯機 VPN 通道連接名稱,如 XXX Office,建議您若是有一個以上的通道設定的話,務必將每一個通道名稱都設為不同,以免混淆

Note: 此通道名稱若是您需要連接其他 VPN 設備(非 FVR9416)時,有一些設備規定此通道名稱要與主控端為相同名稱並做驗證,此通道才會順利聯機開啟!.

Phase2 Encrypt/Auth/Group:　於此顯示加密(DES/3DES)以及驗證(MD5/SHA1)以及群組 Group (1/2/5)等設定模式.
若是您選擇手動(Manual)設定 IPSec 的話,於此將不會顯示 Phase 2 DH 群組

Local Group:　此為顯示本地區域端的 VPN 聯機安全群組設定

Remote Group:　此為顯示遠端的 VPN 聯機安全群組設定

Remote Gateway:　此為設定為欲與遠端 VPN 設備聯機的 IP 位置,請設定為遠端的 VPN 路由器之對外合法 IP 位置或是 Domain Name 等

Tunnel Test:　可以按下連接按鈕-Connect 去驗證此通道的狀態,測試結果將會更新於此狀態上.

Configure:　設定專案包含編輯-Edit 以及刪除圖示



若您按下編輯按鈕- Edit，將會連接到此設定的專案當中,您可以修改其中的設定. 若您選擇按下垃圾桶圖示的話, 所有此通道的設定將會被刪除.

Tunnel(s) Enable and Tunnel(s) Defined: 于此顯示此通道是否開啟 (Tunnel(s) Enable)以及此通道是否已經設定過(Tunnel(s) Defined)..

GroupVPN Status: 群組 VPN 狀態顯示

若您無選擇並設定群組 VPN 模式(GroupVPNs), 此將不顯示出會群組 VPN(GroupVPNs)狀態.

GroupVPN Status

Group Name	Connected Tunnels	Phase2 Enc/Auth/Grp	Local Group	Remote Client	Remote Client Status	Tunnel Test	Config.

Group ID Name: 目前設定聯機 GroupVPNs 通道連接名稱.

Connected Tunnels: 於此顯示已經聯機的 VPNGroups 通道.

Phase2 Encrypt/Auth/Group: 於此顯示加密(DES/3DES)以及驗證(MD5/SHA1)以及群組 Group (1/2/5)等設定模式.
若是您選擇手動(Manual)設定 IPSec 的話,於此將不會顯示 Phase 2 DH 群組

Local Group: 此為顯示本地區域端的群組 VPN 聯機安全群組設定

Remote Client: 此為顯示此 GroupVPN.遠端的 VPN 聯機安全群組設定

Remote Clients Status: 若您按下更多資訊列表(Detail List) 按鈕, 此將會顯示更多有關資訊, 包含群組名稱(Group Name),IP位置(IP Address)以及聯機時間資訊等.

Tunnel Test: 可以按下連接按鈕-Connect 去驗證此通道的狀態,測試結果將會更新於此狀態上.

Config: 如下圖所示,設定項目包含編輯-Edit 以及刪除圖示

若您按下編輯按鈕- Edit ，將會連接到此設定的專案當中,您可以修改其中的設定. 若您選擇按下垃圾桶圖示的話, 所有此通道的設定將會被刪除.

Group VPN Connection List Refresh Close

Group Name	IP address	Connection Time (seconds)

.



Add New Tunnel 新增一條 VPN 通道

Gateway to Gateway-VPN 閘道器對閘道器的設定

透過以下的設定說明,使用者就可以在兩台 **FVR9416** 之間建立一條 **VPN** 通道

Tunnel No.: 當您設定 FVR9416 內建之 VPN 功能時,請選擇您要設定的 Tunnel 通道編號,FVR9416 可支援最高 200VPN 通道設定

Interface: 您可以選擇哪一個介面位置做為此 VPN 通道的節點,一開始的預設 WAN 端共有四個 WAN1~4 可作為此 VPN 通道的使用

Tunnel Name: 設定此通道連接名稱,如 XXX Office,建議您若是有一個以上的通道設定的話,務必將每一個通道名稱都設為不同,以免混淆

Note: 此通道名稱若是您需要連接其他 VPN 設備(非 FVR9416)時,有一些設備規定此通道名稱要與主控端為相同名稱並做驗證,此通道才會順利聯機開啟!.

Enable: 勾選 Enable 選項,將此 VPN 通道開啟. 此項目為預設為啟動 Eanble,當設定完成後,可以再選擇是否啟動通道設定.

Tunnel No. 1
Tunnel Name
Interface WAN1
Enable



Local Group Setup:

Local Security Gateway Type:

區域端群組設定,有五種操作模式專案選擇,分別為:

IP Only-只使用 IP 作為認證

IP + Domain Name(FQDN) Authentication,-IP+網功能變數名稱稱

IP + E-mail Addr.(USER FQDN) Authentication,-IP+電子郵件

Dynamic IP + Domain Name(FQDN) Authentication,-動態 IP 位置+網功能變數名稱稱

Dynamic IP + E-mail Addr.(USER FQDN) Authentication. 動態 IP 位置+電子郵件名稱

此專案的近端閘道安全群組設定**(Local Security Gateway Type)**型態必須與連接遠端的遠端閘道安全群組設定**(Remote Security Gateway Type)**型態相同**.**

(1) IP Only: 若您選擇 IP Only 型態的話, 只有固定填入此 IP 位置可以存取此通道,然後 FVR9416 的 WAN IP 位置,將會自動填入此專案空格內,您不需要在進行額外設定.

Local Security Gateway Type: IP Only
IP address: 192 . 168 . 5 . 86

(2) IP + Domain Name(FQDN) Authentication: 若您選擇 IP +網功能變數名稱稱型態的話,請輸入您所驗證的網功能變數名稱稱以及 IP 位置然後 FVR9416 的 WAN IP 位置,將會自動填入此專案空格內,您不需要在進行額外設定. FQDN 是指主機名稱以及網功能變數名稱稱的結合,也必須存在於 Internet 上可以查詢的到,如 vpn.server.com.此 IP 位置以及網功能變數名稱稱必須與遠端的 VPN 安全閘道器設定型態相同才可以正確連接..

Local Security Gateway Type: IP + Domain Name(FQDN) Authentication
Domain Name:
IP address: 192 . 168 . 5 . 86

(3) IP + E-mail Addr.(USER FQDN) Authentication: 若您選擇 IP 位置加上電子郵件型態的話, 只有固定填入此 IP 位置以及電子郵件位置可以存取此通道,然後 FVR9416 的 WAN IP 位置,將會自動填入此專案空格內,您不需要在進行額外設定.

Local Security Gateway Type: IP + E-mail Addr.(USER FQDN) Authentication
E-mail address: @
IP address: 192 . 168 . 5 . 86

(4) Dynamic IP + Domain Name(FQDN) Authentication: 若是您使用動態 IP 位置連接 FVR9416 時, 您可以選擇此型態連接 VPN, ,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 聯機時, FVR9416 將會開始驗證並回應此 VPN 通道聯機; 若您選擇此型態連接 VPN, 請輸入網功能變數名稱稱即可



Local Security Gateway Type	Dynamic IP + Domain Name(FQDN) Authentication
Domain Name	

(5) Dynamic IP + E-mail Addr.(USER FQDN) Authentication: 若 是您使用動態 IP 位置連接 FVR9416 時, 您可以選擇此型態連接 VPN,使用者不必輸入 IP 位置,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 聯機時, FVR9416 將會開始驗證並回應此 VPN 通道聯機; 若您選擇此型態連接 VPN,請輸入電子郵件認證到 E-Mail 位置空格欄位中即可.

Local Security Gateway Type	Dynamic IP + E-mail Addr.(USER FQDN) Authentication
E-mail address	@

Local Security Group Type

此為設定本地區域端的 VPN 聯機安全群組設定,以下有幾個關於本地區域端設定的專案,請您選擇並設置適當參數:

(1) **IP Address**

此專案為允許此 VPN 通道聯機後,只有輸入此 IP 位置的本地端電腦可以聯機.

Local Security Group Type	IP
IP address	192 . 168 . 1 . 0

以上的設定參考為:當此 VPN 通道聯機後,於 192.168.1.0~255 的此網段的 IP 位置範圍的電腦可以聯機.

(2) **Subnet**

此專案為允許此 VPN 通道聯機後,每一台于此網段的本地端電腦都可以聯機..

Local Security Group Type	Subnet
IP address	192 . 168 . 1 . 0
Subnet Mask	255 . 255 . 255 . 192

以上的設定參考為:當此 VPN 通道聯機後,只有 192.168.1.0,子網路遮罩為 255.255.255.192 的此網段電腦可以與遠端 VPN 聯機

***Remote Group Setup**: 遠程安全 VPN 群組設定.*

Remote Security Gateway Type:

遠端安全群組設定,有五種操作模式專案選擇,分別為:
IP Only-只使用 IP 作為認證
IP + Domain Name(FQDN) Authentication,-IP+網功能變數名稱稱
IP + E-mail Addr.(USER FQDN) Authentication,-IP+電子郵件
Dynamic IP + Domain Name(FQDN) Authentication,-動態 IP 位置+網功能變數名稱稱
Dynamic IP + E-mail Addr.(USER FQDN) Authentication. 動態 IP 位置+電子郵件名稱



此專案的遠端閘道安全群組設定**(Remote Security Gateway Type)**型態必須與連接遠端的近端閘道安全群組設定**(Local Security Gateway Type)**型態相同**.**

(1) IP Only: 若您選擇 IP Only 型態的話，只有固定填入此 IP 位置可以存取此通道，

Remote Security Gateway Type　IP Only
IP address　. . .

若是使用者不曉得遠端客戶的 IP address,則可以透過網功能變數名稱稱轉換 DNS Resolve 來將 DNS 轉成 IP address.並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP address.

Remote Security Gateway Type　IP Only
IP by DNS Resolved

(2) IP + Domain Name(FQDN) Authentication:若您選擇 IP +網功能變數名稱稱型態的話,請輸入 IP 位置以及您所驗證的網功能變數名稱稱 FQDN 是指主機名稱以及網功能變數名稱稱的結合,使用者可以輸入一個符合 FQDN 的網功能變數名稱稱即可.此 IP 位置以及網功能變數名稱稱必須與遠端的 VPN 安全閘道器設定型態相同才可以正確連接.

Remote Security Gateway Type　IP + Domain Name(FQDN) Authentication
IP address　. . .
Domain Name

若是使用者不曉得遠端的 IP address,則可以透過網功能變數名稱稱轉換 DNS Resolve 來將 DNS 轉成 IP address.此網功能變數名稱稱必須存在 Internet 上可以查詢的到.並且在設定完成後在 Summary 的遠端閘道下面自動顯示出相對應的 IP address.

Remote Security Gateway Type　IP + Domain Name(FQDN) Authentication
IP by DNS Resolved
Domain Name

(3) IP + E-mail Addr.(USER FQDN) Authentication: 若您選擇 IP 位置加上電子郵件型態的話，只有固定填入此 IP 位置以及電子郵件位置可以存取此通道，

Remote Security Gateway Type　IP + E-mail Addr.(USER FQDN) Authentication
IP address　. . .
E-mail address　@

若是使用者不曉得遠端客戶的 IP address,則可以透過網功能變數名稱稱轉換 DNS Resolve 來將 DNS 轉成 IP address.並且在設定



完成後在 Summary 的遠端閘道下面顯示出相對應的 IP address.

Remote Security Gateway Type	IP + E-mail Addr.(USER FQDN) Authentication
IP by DNS Resolved	
E-mail address	@

(4) Dynamic IP + Domain Name(FQDN) Authentication: 若是您使用動態 IP 位置連接 FVR9416 時,您可以選擇動態 IP 位置加上主機名稱以及網功能變數名稱稱的結合

Remote Security Gateway Type	Dynamic IP + Domain Name(FQDN) Authentication
Domain Name	

(5) Dynamic IP + E-mail Addr.(USER FQDN) Authentication: 若是您使用動態 IP 位置連接 FVR9416 時, 您可以選擇此型態連接 VPN,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 聯機時, FVR9416 將會開始驗證並回應此 VPN 通道聯機; 請輸入電子郵件認證到 E-Mail 位置空格欄位中

Remote Security Gateway Type	Dynamic IP + E-mail Addr.(USER FQDN) Authentication
E-mail address	@

Remote Security Group Type:

此為設定本地區域端的 VPN 聯機安全群組設定,以下有幾個關於本地區域端設定的專案,請您選擇並設置適當參數:

(1) IP Address

此專案為允許此 VPN 通道聯機後,只有輸入此 IP 位置的本地端電腦可以聯機.

Remote Security Group Type	IP
IP address	0 . 0 . 0 . 0

以上的設定參考為:當此 VPN 通道聯機後,於 192.168.1.0~255 的此網段的 IP 位置範圍的電腦可以聯機.

(2)Subnet

此專案為允許此 VPN 通道聯機後,每一台于此網段的本地端電腦都可以聯機..

Remote Security Group Type	Subnet
IP address	. . .
Subnet Mask	255 . 255 . 255 . 0

以上的設定參考為:當此 VPN 通道聯機後,只有 192.168.1.0,子網路遮罩為 255.255.255.192 的此網段電腦可以與遠端 VPN 聯機

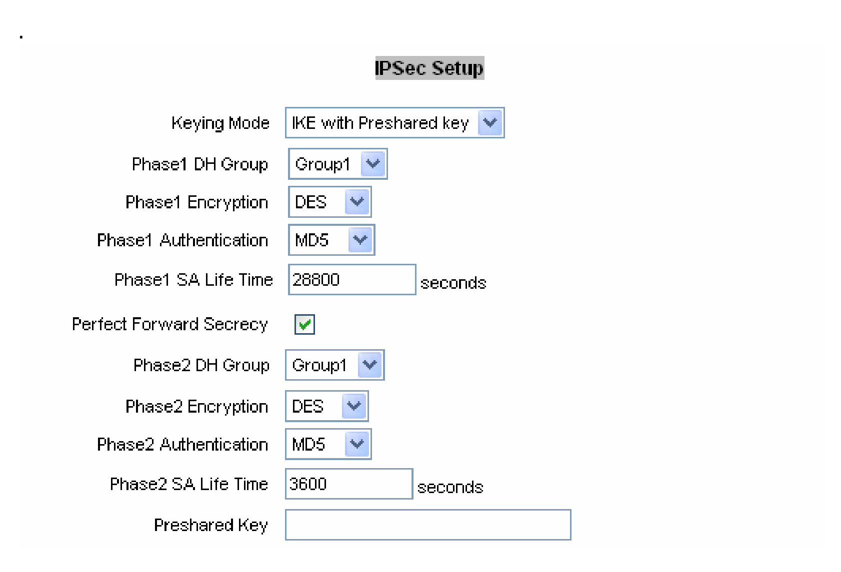


IPSec Setup

若是任何加密機制存在的話, 此兩個 VPN 通道的加密機制必須要相同才可以將此通道連接,並於傳輸資料中加上標準的 IPSec 密鑰,於此我們稱為加密密鑰 “key” . FVR9416 提供了以下二種加密管理模式 Key Management,分別為手動(**Manual**) 以及 IKE 自動加密模式- **IKE with Preshared Key (automatic)**如下圖所示..

Key Management:

.



IKE with Preshared Key (automatic): 此選項設定為當您設定此VPN通道使用何種加密模式以及驗證模式後,必須設定一組交換密碼,並請注意此參數必須與遠端的交換密碼參數相同;設定的方式有自動 **Auto (IKE)**或是手動 **Manual.**設定二種**:**於設定時請您選擇其中一種設定方式即可!.

Phase1/Phase2 DH Group:

於此選項可以選擇採用 Diffie-Hellman 群組方式: Group1(768 bits) 或是 Group2(1,024 bits)/Group5(1,536 bits).

Phase1/Phase2 Encryption:
此加密選項設定為設定此 VPN 通道使用何種加密模式,並請注意設置此參數必須與遠端的加密參數相同:
DES: 64-位元加密模式 **3DES:**.128-位元加密模式.

Phase1/Phase2 Authentication:
此驗證選項設定為設定此 VPN 通道使用何種驗證模式,並請注意設置此參數必須與遠端的驗證模式參數相同:
“MD5”/“SHA”.

Phase1 SA Lifetime 設定為此交換密碼的有效時間,系統預設值為 28800 秒(8 小時),於此有效時間內的 VPN 聯機,系統會自動的將於有效時間後,自動的生成其他的交換密碼以確保安全.

Phase2 SA Lifetime 設定為此交換密碼的有效時間,系統預設值為 3600 秒(1 小時),於此有效時間內的 VPN 聯機,系統會自動的將於有效時間



後,自動的生成其他的交換密碼以確保安全.

Keying Mode: Manual
Incoming SPI
Outgoing SPI
Encryption: DES
Authentication: MD5
Encryption Key
Authentication Key

Manual: 手動方式

若您選擇手動模式 **Manual** 的話,此提供您自訂加密密鑰 ,而此密鑰不需經過任何交握(negotiation).

Manual 為手動方式設定交換密碼,於此分成加密密碼"**Encryption KEY**"以及驗證密碼"**Authentication KEY**"二種,您可以輸入數位或是文字的交換密碼,系統將會自動的將您輸入的數位或是文字的交換密碼自動轉成 VPN 通道連接時的交換密碼與驗證機制;此數位或是文字的交換密碼最高可輸入 23 個文字組合

Incoming &outgoing SPI: 另外還需要設定"**Inbound SPI"**的交換字串以及"**Outbound SPI"** 交換字串,此字串必須與遠端 VPN 設備連接時相同;於此的 Inbound SPI 設定參數,您必須在遠端的 VPN 設備的 Outbound SPI 設定相同字串,而於本地端的 Outbound SPI 設定字串,也必須與在遠端的 VPN 設備的 Inbound SPI 設定相同字串

***Advanced*-(進階作業模式)-**只供給使用自動交換密鑰模式使用**(IKE With Preshareed Key Only)**

Advanced settings are only for IKE with Preshared Key mode of IPSec.

Advance Mode(進階作業模式)

Aggressive Mode
Compress (Support IP Payload Compression Protocol(IPComp))
Keep-Alive
AH Hash Algorithm: >MD5
NetBIOS broadcast
Dead Peer Detection (DPD) Interval 10 seconds

在 FVR9416 的進階設定項目中,分別有主要模式 **Main Mode** 以及 進階模式 **Aggressive Mode**, Main mode 是 FVR9416 的預設 VPN 作業模式而且與大多數的其他 VPN 設備使用連接方式為相同;另外 Aggressive mode 大多為遠端的設備採用,如使用動態 IP 連接時,為了加強其安全控管機制,

Compress:
若選擇此項目勾選,則連接的VPN通道中FVR9416 支援IP表頭型態的壓縮(IP Payload compression Protocol).

Keep-Alive:
若選擇此項目勾選,則連接的 VPN 通道中會持續保持此條 VPN 連接不會中斷,此使用多為分公司遠端節點對總部的連接使用,或是無固定 IP 位置的遠端使用.

AH Hash Algorithm:
AH (Authentication Header) 驗證表頭封包格式,可選擇 MD5/DSHA-1

NetBIOS Broadcast:
若選擇此項目勾選,則連接的VPN通道中會讓NetBIOS 廣播封包通過.,有助於微軟的系統網路芳鄰等連接容易,但是相對的佔用此 VPN 通道的流量就會加大!

Dead Peer Detection(DPD):

若選擇此項目勾選,則連接的VPN通道中會定期的傳送HELLO/ACK 訊息封包來偵測是否 VPN 通道的兩端仍有聯機存在.當有一端斷線則 FVR9416 會自動斷線,然後再建立新聯機.使用者可以選擇每一次 DPD 訊息封包傳遞的時間,預設值為 10 秒.

Client to Gateway

VPN 用戶端對閘道器的設定

透過以下的設定說明,使用者就可以在用戶端與近端使用 FVR9416 之間建立一條 VPN 通道.管理者可以選擇這一條 VPN 通道在用戶端是只供一個客戶所使用(Tunnel)或者是由一群客戶所使用(Group VPN).若由一群客戶所使用則可以節省個別設定遠端的客戶,只需設定的一條通道供一組客戶所使用,以節省設定時的麻煩.

In Tunnel condition-在 Tunnel 的情況:

Tunnel No.: 當您設定 FVR9416 內建之 VPN 功能時,請選擇您要設定的 Tunnel 通道編號,FVR9416 可支援最高 200VPN 通道設定

Interface: 您可以選擇哪一個介面位置做為此 VPN 通道的節點,一開始的預設 WAN 端共有四個 WAN1~4 可作為此 VPN 通道的使用.

Tunnel Name: 設定此通道連接名稱,如 XXX Office,建議您若是有一個以上的通道設定的話,務必將每一個通道名稱都設為不同,以免混淆

Note: 此通道名稱若是您需要連接其他 VPN 設備(非 FVR9416)時,有一些設備規定此通道名稱要與主控端為相同名稱並做驗證,此通道才會順利聯機開啟!.



Enable:

勾選 Enable 選項,將此 VPN 通道開啟. 此項目為預設為啟動 Eanble, 當設定完成後可以再選擇是否啟動通道設定.

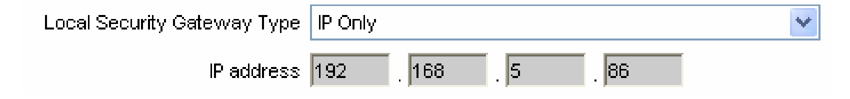
Tunnel No. 1
Tunnel Name
Interface WAN1
Enable

Local Group Setup:

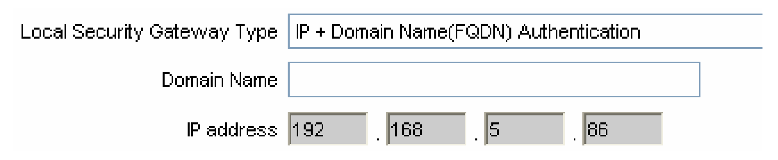
區域端群組設定,有五種操作模式專案選擇,分別為:
IP Only-只使用 IP 作為認證
IP + Domain Name(FQDN) Authentication,-IP+網功能變數名稱稱
IP + E-mail Addr.(USER FQDN) Authentication,-IP+電子郵件
Dynamic IP + Domain Name(FQDN) Authentication,-動態 IP 位置+網功能變數名稱稱
Dynamic IP + E-mail Addr.(USER FQDN) Authentication. 動態 IP 位置+電子郵件名稱

此專案的近端閘道安全群組設定**(Local Security Gateway Type)**型態必須與連接遠端的遠端閘道安全群組設定**(Remote Security Gateway Type)**型態相同**.**

(1) IP Only: 若您選擇 IP Only 型態的話, 只有固定填入此 IP 位置可以存取此通道,然後 FVR9416 的 WAN IP 位置,將會自動填入此專案空格內,您不需要在進行額外設定.



(2) IP + Domain Name(FQDN) Authentication:若您選擇 IP +網功能變數名稱稱型態的話,請輸入您所驗證的網功能變數名稱稱以及 IP 位置然後 FVR9416 的 WAN IP 位置,將會自動填入此專案空格內,您不需要在進行額外設定. FQDN 是指主機名稱以及網功能變數名稱稱的結合,也必須存在於 Internet 上可以查詢的到,如 vpn.server.com. 此 IP 位置以及網功能變數名稱稱必須與遠端的 VPN 安全閘道器設定型態相同才可以正確連接.



(3) IP + E-mail Addr.(USER FQDN) Authentication: 若您選擇 IP 位置加上電子郵件型態的話, 只有固定填入此 IP 位置以及電子郵件位置可以存取此通道,然後 FVR9416 的 WAN IP 位置,將會自動填入此專案空格內,您不需要在進行額外設定



Local Security Gateway Type: IP + E-mail Addr.(USER FQDN) Authentication

E-mail address @

IP address 192 . 168 . 5 . 86

(4) Dynamic IP + Domain Name(FQDN) Authentication:

若是您使用動態 IP 位置連接 FVR9416 時, 您可以選擇此型態連接 VPN, ,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 聯機時, FVR9416 將會開始驗證並回應此 VPN 通道聯機; 若您選擇此型態連接 VPN,請輸入網功能變數名稱稱即可

Local Security Gateway Type: Dynamic IP + Domain Name(FQDN) Authentication

Domain Name

(5) Dynamic IP + E-mail Addr.(USER FQDN) Authentication: 若是您使用動態 IP 位置連接 FVR9416 時, 您可以選擇此型態連接 VPN, 使用者不必輸入 IP 位置, 當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 聯機時, FVR9416 將會開始驗證並回應此 VPN 通道聯機; 若您選擇此型態連接 VPN,請輸入電子郵件認證到 E-Mail 位置空格欄位中即可

Local Security Gateway Type: Dynamic IP + E-mail Addr.(USER FQDN) Authentication

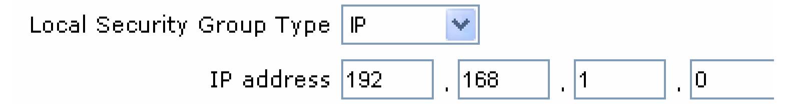
E-mail address @

Local Security Gateway Type:

此為設定本地區域端的 VPN 聯機安全群組設定,以下有幾個關於本地區域端設定的專案,請您選擇並設置適當參數:

(1)IP Address

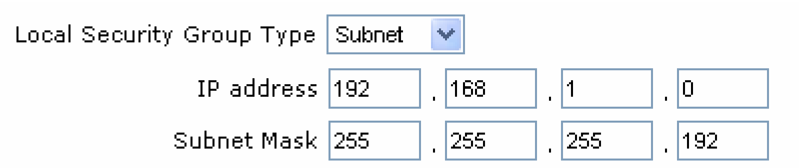
此專案為允許此 VPN 通道聯機後,只有輸入此 IP 位置的本地端電腦可以聯機.



以上的設定參考為:當此 VPN 通道聯機後,於 192.168.1.0~255 的此網段的 IP 位置範圍的電腦可以聯機.

(2)Subnet

此專案為允許此 VPN 通道聯機後,每一台于此網段的本地端電腦都可以聯機..



以上的設定參考為:當此 VPN 通道聯機後,只有 192.168.1.0,子網路遮罩為 255.255.255.192 的此網段電腦可以與遠端 VPN 聯機此專案為允許此 VPN 通道聯機後,只有輸入此 IP 位置範圍的本地 端電 腦可以聯機



***Remote Client Setup**: 遠程用戶端設定*

Remote Client: 遠端用戶端設定,有五種操作模式專案選擇,分別為:
IP Only-只使用 IP 作為認證
IP + Domain Name(FQDN) Authentication,-IP+網功能變數名稱稱
IP + E-mail Addr.(USER FQDN) Authentication,-IP+電子郵件
Dynamic IP + Domain Name(FQDN) Authentication,-動態 IP 位置+網功能變數名稱稱
Dynamic IP + E-mail Addr.(USER FQDN) Authentication. 動態 IP 位置+電子郵件名稱

此專案的遠端閘道安全群組設定**(RemoteSecurity Gateway Type)**型態必須與連接遠端的近端閘道安全群組設定**(Local Security Gateway Type)**型態相同**.**

(1) IP Only: 若您選擇 IP Only 型態的話，只有固定填入此 IP 位置可以存取此通道,

Remote Security Gateway Type | IP Only
IP address | . . .

若是使用者不曉得遠端客戶的 IP address,則可以透過網功能變數名稱稱轉換 DNS Resolve 來將 DNS 轉成 IP address.並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP address.

Remote Security Gateway Type | IP Only
IP by DNS Resolved |

(2) IP + Domain Name(FQDN) Authentication:若您選擇 IP +網功能變數名稱稱型態的話,請輸入 IP 位置以及您所驗證的網功能變數名稱稱~~然後~~FQDN 是指主機名稱以及網功能變數名稱稱的結合,使用者可以輸入一個符合 FQDN 的網功能變數名稱稱即可.此 IP 位置以及網功能變數名稱稱必須與遠端的 VPN 安全閘道器設定型態相同才可以正確連接.

Remote Security Gateway Type | IP + Domain Name(FQDN) Authentication
IP address | . . .
Domain Name |

若是使用者不曉得遠端的 IP address,則可以透過網功能變數名稱稱轉換 DNS Resolve 來將 DNS 轉成 IP address.此網功能變數名稱稱必須存在 Internet 上可以查詢的到.並且在設定完成後在 Summary 的遠端閘道下面自動顯示出相對應的 IP address.

Remote Security Gateway Type | IP + Domain Name(FQDN) Authentication
IP by DNS Resolved |
Domain Name |

(3) IP + E-mail Addr.(USER FQDN) Authentication: 若您選擇 IP



位置加上電子郵件型態的話，只有固定填入此 IP 位置以及電子郵件位置可以存取此通道

Remote Security Gateway Type: IP + E-mail Addr.(USER FQDN) Authentication
IP address: . . .
E-mail address: @

若是使用者不曉得遠端客戶的 IP address,則可以透過網功能變數名稱稱轉換 DNS Resolve 來將 DNS 轉成 IP address.並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP address.

Remote Security Gateway Type: IP + E-mail Addr.(USER FQDN) Authentication
IP by DNS Resolved
E-mail address: @

(4) **Dynamic IP + Domain Name(FQDN) Authentication:** 若是您使用動態 IP 位置連接 FVR9416 時,您可以選擇動態 IP 位置加上主機名稱以及網功能變數名稱稱的結合

Remote Security Gateway Type: Dynamic IP + Domain Name(FQDN) Authentication
Domain Name

(5) **Dynamic IP + E-mail Addr.(USER FQDN) Authentication:** 若是您使用動態 IP 位置連接 FVR9416 時，您可以選擇此型態連接 VPN,當遠端的 VPN 閘道要求與 FVR9416 作為 VPN 聯機時，FVR9416 將會開始驗證並回應此 VPN 通道聯機；請輸入電子郵件認證到 E-Mail 位置空格欄位中

Remote Security Gateway Type: Dynamic IP + E-mail Addr.(USER FQDN) Authentication
E-mail address: @

IPSec Setup

若是任何加密機制存在的話，此兩個 VPN 通道的加密機制必須要相同才可以將此通道連接,並於傳輸資料中加上標準的 IPSec 密鑰,於此我們稱為加密密鑰 “key” . FVR9416 提供了以下二種加密管理模式,分別為手動(**Manual**）以及 IKE 自動加密模式- **IKE with Preshared Key (automatic)**如下圖所示..

Key Management: 提供了以下二種加密管理模式,分別為手動(**Manual**) 以及 IKE 自動加密模式- **IKE with Preshared Key (automatic)**

IPSec Setup

Keying Mode	IKE with Preshared key	
Phase1 DH Group	Group1	
Phase1 Encryption	DES	
Phase1 Authentication	MD5	
Phase1 SA Life Time	28800	seconds
Perfect Forward Secrecy	☑	
Phase2 DH Group	Group1	
Phase2 Encryption	DES	
Phase2 Authentication	MD5	
Phase2 SA Life Time	3600	seconds
Preshared Key		

IKE with Preshared Key (automatic): 於 **Auto (IKE),** 選項中,您必須輸入一組交換密碼於 **"Pre-shared Key"** 的欄位中,在此的範例設定為 **test**,您可以輸入數位或是文字的交換密碼,系統將會自動的將您輸入的數位或是文字的交換密碼自動轉成VPN通道連接時的交換密碼與驗證機制;此數位或是文字的交換密碼最高可輸入 23 個文字組合.
另外您可以選擇 **PFS**(Perfect Forward Secrecy)以便作為交換密碼機制,若您將PFS選項勾選後,記得另外的遠端VPN設備或是VPN Client 也要將 PFS 功能開啟.

Phase1/Phase2 DH Group:

於此選項可以選擇採用 Diffie-Hellman 群組方式: Group1 或是 Group2/Group5.

Phase1/Phase2 Encryption:
此加密選項設定為設定此 VPN 通道使用何種加密模式,並請注意設置此參數必須與遠端的加密參數相同:
DES: 64-位元加密模式 **3DES:**.128-位元加密模式.

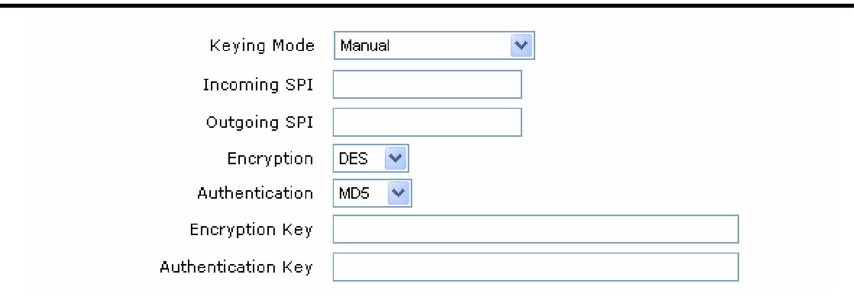
Phase1/Phase2 Authentication:
此驗證選項設定為設定此 VPN 通道使用何種驗證模式,並請注意設置此參數必須與遠端的驗證模式參數相同:
"MD5"/"SHA".
.

Phase1 SA Lifetime 設定為此交換密碼的有效時間,系統預設值為 28800 秒(8 小時),於此有效時間內的 VPN 聯機,系統會自動的將於有效時間後,自動的生成其他的交換密碼以確保安全.

Phase2 SA Lifetime 設定為此交換密碼的有效時間,系統預設值為 3600 秒(1 小時),於此有效時間內的 VPN 聯機,系統會自動的將於有效時間後,自動的生成其他的交換密碼以確保安全.

Manual





Manual: 手動方式

若您選擇手動模式 **Manual** 的話,此提供您自訂加密密鑰,而此密鑰不需經過任何交握(negotiation).

Manual 為手動方式設定交換密碼,於此分成加密密碼“**Encryption KEY**”以及驗證密碼“**Authentication KEY**”二種,您可以輸入數位或是文字的交換密碼,系統將會自動的將您輸入的數位或是文字的交換密碼自動轉成 VPN 通道連接時的交換密碼與驗證機制;此數位或是文字的交換密碼最高可輸入 23 個文字組合.

另外還需要設定“**Inbound SPI”**的交換字串以及“**Outbound SPI”** 交換字串,此字串必須與遠端 VPN 設備連接時相同;於此的 Inbound SPI 設定參數,您必須在遠端的 VPN 設備的 Outbound SPI 設定相同字串,而於本地端的 Outbound SPI 設定字串,也必須與在遠端的 VPN 設備的 Inbound SPI 設定相同字串

***Advanced*- IKE Preshared Key Only(進階作業模式)-**只供給使用自動交換密鑰模式使用

Advanced settings are only for IKE with Preshared Key mode of IPSec.

Advance Mode(進階作業模式)

- ☐ Aggressive Mode
- ☐ Compress (Support IP Payload Compression Protocol(IPComp))
- ☐ Keep-Alive
- ☐ AH Hash Algorithm >MD5
- ☐ NetBIOS broadcast
- ☐ Dead Peer Detection (DPD) Interval 10 seconds

在 FVR9416 的進階設定項目中, 分別有主要模式 **Main Mode** 以及 進階模式 **Aggressive Mode**,Main mode 是 FVR9416 的預設 VPN 作業模式而且與大多數的其他 VPN 設備使用連接方式為相同;另外 Aggressive mode 大多為遠端的設備採用,如使用動態 IP 連接時,為了加強其安全控管機制,.

Compress:

若選擇此項目勾選,則連接的 VPN 通道中 FVR9416 支援 IP 表頭型態的



壓縮(IP Payload compression Protocol).

Keep-Alive:
若選擇此項目勾選,則連接的 VPN 通道中會持續保持此條 VPN 連接不會中斷,此使用多為分公司遠端節點對總部的連接使用,或是無固定 IP 位置的遠端使用.

AH Hash Algorithm:
AH (Authentication Header) 驗證表頭封包格式,可選擇 MD5/DSHA-1

NetBIOS Broadcast:
若選擇此項目勾選,則連接的 VPN 通道中會讓 NetBIOS 廣播封包通過.,有助於微軟的系統網路芳鄰等連接容易,但是相對的佔用此 VPN 通道的流量就會加大!

Dead Peer Detection(DPD):

若選擇此項目勾選,則連接的 VPN 通道中會定期的傳送 HELLO/ACK 訊息封包來偵測是否 VPN 通道的兩端仍有聯機存在.當有一端斷線則 FVR9416 會自動斷線,然後再建立新聯機.使用者可以選擇每一次 DPD 訊息封包傳遞的時間,預設值為 10 秒.

In Group VPN Condition: 在 Group VPN 的情況

Group No.: 最多可以設定兩組 Group VPN.

Interface: 您可以選擇哪一個介面位置做為此 VPN 通道的節點,一開始的預設 WAN 端共有四個 WAN1~4 可作為此 VPN 通道的使用.

Group Name: 設定此通道連接名稱,如 XXX Office,建議您若是有一個以上的通道設定的話,務必將每一個通道名稱都設為不同,以免混淆

Note: 此通道名稱若是您需要連接其他 VPN 設備(非 FVR9416)時,有一些設備規定此通道名稱要與主控端為相同名稱並做驗證,此通道才會順利聯機開啟!.

Enable: 勾選 Enable 選項,將此 VPN 通道開啟. 此項目為預設為啟動 Eanble,當設定完成後可以再選擇是否啟動通道設定.

Tunnel No. 1
Tunnel Name
Interface WAN1
Enable

Local Group Setup:

Local Security Group Type:

此為設定本地區域端的 VPN 聯機安全群組設定,以下有幾個關於本地區域端設定的專案,請您選擇並設置適當參數:

(1)IP Address
此專案為允許此 VPN 通道聯機後,只有輸入此 IP 位置的本地端電腦可以聯機.



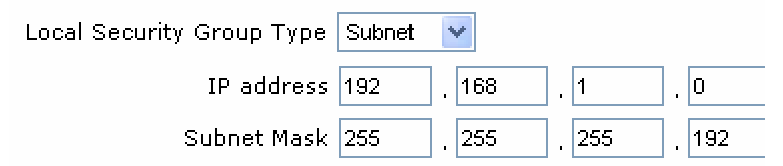
Local Security Group Type IP

IP address 192 . 168 . 1 . 0

以上的設定參考為:當此 VPN 通道聯機後,於 192.168.1.0~255 的此網段的 IP 位置範圍的電腦可以聯機.

(2)Subnet

此專案為允許此 VPN 通道聯機後,每一台于此網段的本地端電腦都可以聯機..



以上的設定參考為:當此 VPN 通道聯機後,只有 192.168.1.0,子網路遮罩為 255.255.255.192 的此網段電腦可以與遠端 VPN 聯機

***Remote Client Setup**: 遠程用戶端設定*

Remote Client: *遠端用戶端設定*,有三種操作模式專案選擇,分別為:

Domain Name(FQDN),-網功能變數名稱稱
E-mail Address(USER FQDN),- 電子郵件名稱
Microsoft XP/2000 VPN Client,- 微軟 XP/2000 VPN 用戶端

(1) Domain Name(FQDN):

若您選擇網功能變數名稱稱型態的話,請輸入您所驗證的網功能變數名稱稱.FQDN 是指主機名稱以及網功能變數名稱稱的結合,也必須存在於 Internet 上可以查詢的到,如 vpn.server.com.此網功能變數名稱稱必須與用戶端的近端設定型態相同才可以正確連接

Remote Client Domain Name(FQDN)
Domain Name

(2) E-mail Addr.(USER FQDN):

若您選擇電子郵件型態的話, 只有固定填入此電子郵件位置可以存取此通道

Remote Client E-mail Address(USER FQDN)
E-mail address @

(3) Microsoft XP/2000 VPN Client:

若您選擇微軟 XP/2000 VPN 用戶端型態的話,您不需要在進行額外設定.

Remote Client Microsoft XP/2000 VPN Client



IPSec Setup

若是任何加密機制存在的話, 此兩個 VPN 通道的加密機制必須要相同才可以將此通道連接,並於傳輸資料中加上標準的 IPSec 密鑰,於此我們稱為加密密鑰 “key”．FVR9416 提供了以下二種加密管理模式,分別為手動(**Manual**）以及 IKE 自動加密模式- **IKE with Preshared Key (automatic).**在選擇 Group VPN 的情況之下或者是在遠端閘道安全型態 Remote Security Gateway Type 中使用動態位置 IP 時,Aggressive mode 會自動啟動,沒有手動 Manual 模式**.**

Key Management:

加密管理模式,IKE 自動加密模式- **IKE with Preshared Key (automatic).**

Keying Mode:	IKE with Preshared key
Phase1 DH Group	Group1
Phase1 Encryption	DES
Phase1 Authentication	MD5
Phase1 SA Life Time	28800
Perfect Forward Secrecy	☑
Phase2 DH Group	Group1
Phase2 Encryption	DES
Phase2 Authentication	MD5
Phase2 SA Life Time	3600
Preshared Key	

於 **Auto (IKE),** 選項中,您必須輸入一組交換密碼於 “**Pre-shared Key”** 的欄位中,在此的範例設定為 **test**,您可以輸入數位或是文字的交換密碼,系統將會自動的將您輸入的數位或是文字的交換密碼自動轉成 VPN 通道連接時的交換密碼與驗證機制;此數位或是文字的交換密碼最高可輸入 23 個文字組合.

另外您可以選擇 **PFS**(Perfect Forward Secrecy)以便作為交換密碼機制,若您將 PFS 選項勾選後,記得另外的遠端 VPN 設備或是 VPN Client 也要將 PFS 功能開啟.

Phase1/Phase2 DH Group:

於此選項可以選擇採用 Diffie-Hellman 群組方式: Group1 或是 Group2/Group5.

Phase1/Phase2 Encryption:

此加密選項設定為設定此 VPN 通道使用何種加密模式,並請注意設置此參數必須與遠端的加密參數相同:

DES: 64-位元加密模式 **3DES:**.128-位元加密模式.

Phase1/Phase2 Authentication:

此驗證選項設定為設定此 VPN 通道使用何種驗證模式,並請注意設置此參數必須與遠端的驗證模式參數相同:

“**MD5”/**“**SHA”**.



.

Phase1 SA Lifetime 設定為此交換密碼的有效時間,系統預設值為 28800 秒(8 小時),於此有效時間內的 VPN 聯機,系統會自動的將於有效時間後,自動的生成其他的交換密碼以確保安全.

Phase2 SA Lifetime 設定為此交換密碼的有效時間,系統預設值為 3600 秒(1 小時),於此有效時間內的 VPN 聯機,系統會自動的將於有效時間後,自動的生成其他的交換密碼以確保安全

Advanced-IKE Preshareed Key Only

Advanced settings are only for IKE with Preshared Key mode of IPSec.

Advance Mode: (進階作業模式)

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm MD5
- NetBIOS broadcast

在 FVR9416 的進階設定項目中,分別有 **Main** Mode 以及 **Aggressive**. 模式, Main mode 是 FVR9416 的預設 VPN 作業模式而且與大多數的其他 VPN 設備使用連接方式為相同;另外 Aggressive mode 大多為遠端的設備採用,如使用動態 IP 連接時,為了加強其安全控管機制.在選擇 Group VPN 時,Aggressive mode 會自動啟動.

Compress:
若選擇此項目勾選,則連接的 VPN 通道中 FVR9416 支援 IP 表頭型態的壓縮(IP Payload compression Protocol).

Keep-Alive:
若選擇此項目勾選,則連接的 VPN 通道中會持續保持此條 VPN 連接不會中斷,此使用多為分公司遠端節點對總部的連接使用,或是無固定 IP 位置的遠端使用.

AH Hash Algorithm:
AH (Authentication Header) 驗證表頭封包格式,可選擇 MD5/DSHA-1

NetBIOS Broadcast:
若選擇此項目勾選,則連接的 VPN 通道中會讓 NetBIOS 廣播封包通過., 有助於微軟的系統網路芳鄰等連接容易,但是相對的佔用此 VPN 通道的流量就會加大!

PPTP

當遠端使用者在建立 VPN 通道聯機時,所使用的協定方式並不是 IPSec 協定的時候,FVR9416 提供支援 Window XP/2000 的 PPTP 點對點通道協定,讓遠端使用此種協定建立 VPN 聯機.

.



Enable PPTP Server: 當使用者勾選後即可以啟動點對點隧道協定 PPTP 伺服器.

PPTP IP Address Range: 請輸入近端 PPTP IP 位址的範圍,其目的是要給遠端的使用者一個可進入近端網路的入口 IP.輸入起始範圍 Range Start:請在最後一欄輸入數值.輸入結束範圍 Range End: 請在最後一欄數入數值.

User Name: 目的為確認遠端使用者的身分,需輸入使用者名稱與密碼,提供近端伺服器作確認.

New Password 請輸入遠端使用者的名稱

Confirm New Password: 請再次確認輸入遠端使用者新的帳號密碼

Add to list: 新增或刪除輸入的帳號與密碼

Delete selected User:	增加到開啟使用者
Connection List:	顯示出使用 PPTP 伺服器通道的使用相關資訊.
User Name:	聯機建立後的遠端使用者名稱
Remote Address:	聯機建立後的遠端使用者的 IP 位置
PPTP IP Address:	聯機建立後,近端 PPTP 伺服器的 IP 位置
Refresh:	按下此按鈕"Refresh"立即刷新畫面
Apply:	按下此按鈕"Apply"即會儲存剛才所變動的修改設定內容參數..
Cancel	按下此按鈕"Cancel"即會清除剛才所變動的修改設定內容參數,但是必須於 Apply 儲存動作之前才會有效

VPN Pass Through -VPN 透通

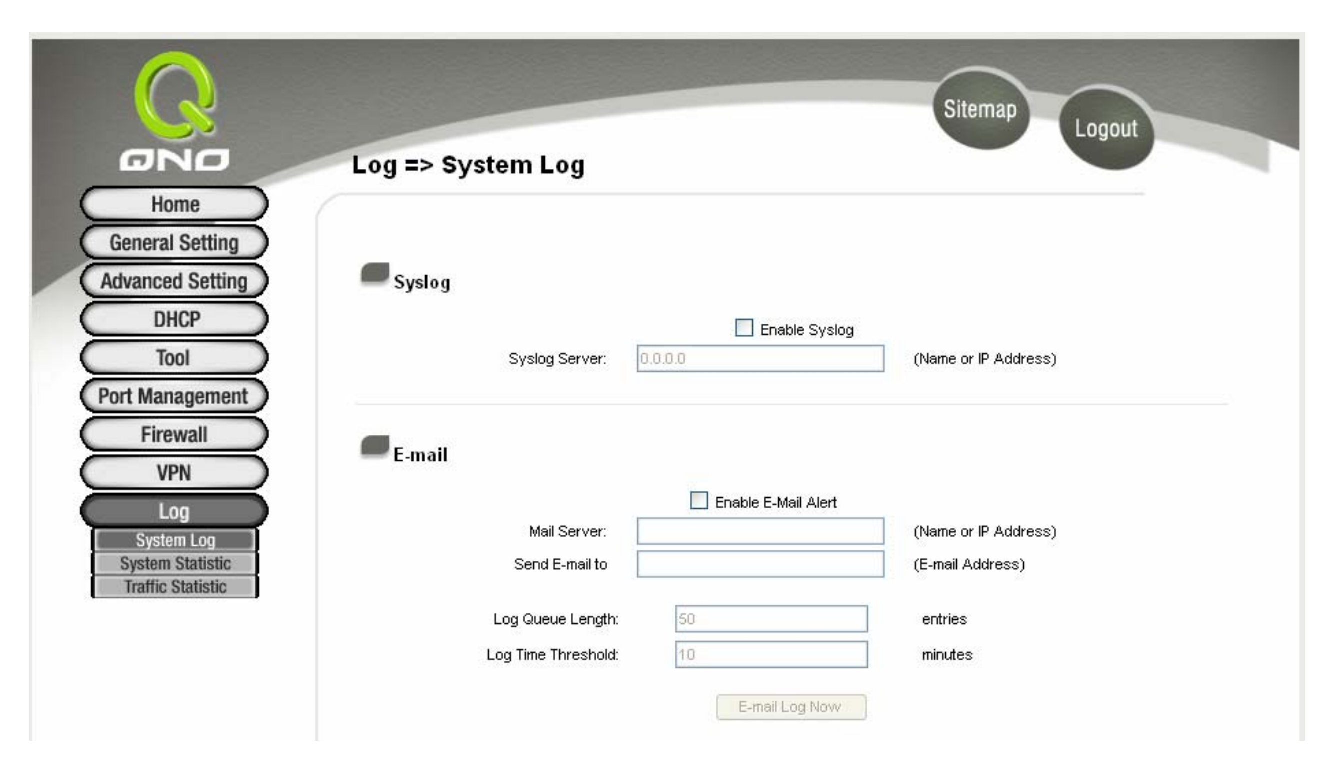
IPSec Pass Through:	若是選擇 **Enable** 的話,則允許 PC 端使用 VPN- IPSec 封包穿透 FVR9416 以便與外部 VPN 設備聯機



PPTP Pass Through:	若是選擇 **Enable** 的話,則允許 PC 端使用 VPN-PPTP 封包穿透 FVR9416 以便與外部 VPN 設備聯機
L2TP Pass Through:	若是選擇 **Enable** 的話,則允許 PC 端使用 VPN-L2TP 封包穿透 FVR9416 以便與外部 VPN 設備聯機

Log 日誌

System Log-系統日誌



FVR9416 系統日誌(System Log)提供三種功能項目,分別為- **Syslog, E-mail** and **Log Setting.**

Syslog 系統日誌

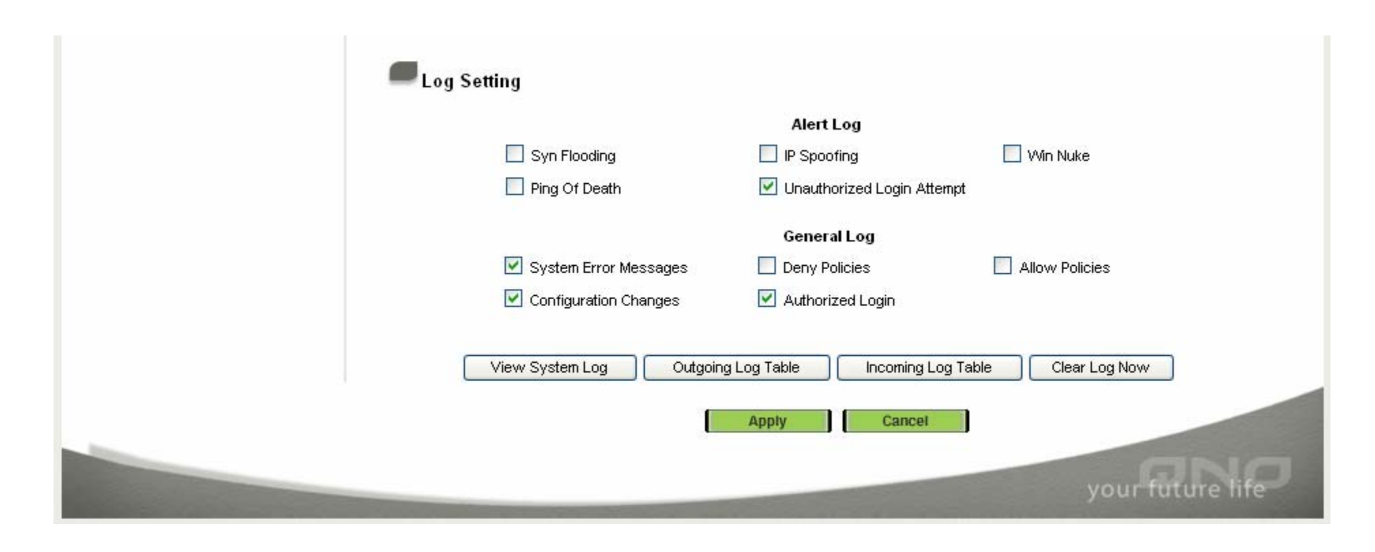
Enable Syslog:	若是此選項勾選的話, Syslog 功能將被開啟
Syslog Server:	FVR9416 提供了外部 Syslog 伺服器收集系統資訊功能. Syslog 為一項工業標準通訊協定,於網路上動態擷取有關的系統資訊. FVR9416 的 Syslog 提供了包含動作中的聯機來源位置(source IP Address)與目地(destination IP Address)位置, 服務編號(Port Number)以及型態(IP service), 輸入 Syslog 伺服器名稱或是 IP 位置於” **Syslog Server”** 的空格欄位內.



E-mail

Enable E-Mail Alert:	若是此選項勾選的話, 電子郵件告警(E-Mail Alert)將會被開啟
Mail Server	若您希望所有的 Log 電子郵件都可以寄出的話,請於此輸入電子郵件伺服器的名稱或是 IP 位置,如 mail.abc.com
Send E-mail To:	此為設定 Log 收件人電子郵件信箱,如 abc@mail.abc.com
Log Queue Length (entries):	自訂 Log entries 數量,系統預設為 50 個 entries. 當到達此數量時,FVR9416 將會自動 Mail 傳送 Log.
Log Time Threshold (minutes):	自訂傳送 Log 間隔時間,系統預設為 10 分鐘. 當到達此時間時,FVR9416 將會自動 Mail 傳送此 Log. FVR9416 將會自動判別當 entries 數量或是間隔時間哪一個參數先到達,就 Mail 傳送 Log 訊息給管理者.
E-mail Log Now:	使用管理者可以直接于此按鈕傳送 Log.

Log Setting 系統日誌設定



Alert Log-選擇需要告警的內容

FVR9416 提供了包含以下的告警內容訊息,您只要打勾點選即可. Syn Flooding, IP Spoofing, Win Nuke, Ping of Death / Unauthorized Login Attempt.

Syn Flooding:	It will cause servers to stop responding to requests of opening new connections with clients
IP Spoofing:	It is used to gain unauthorized access to PCs.



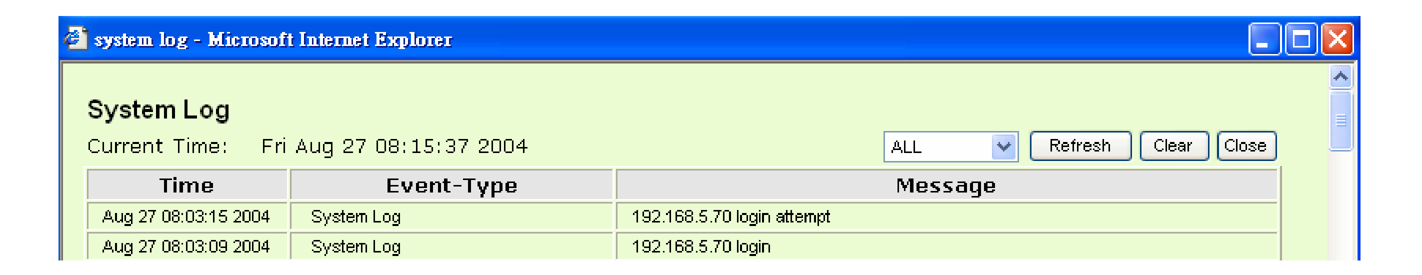
Win Nuke:	It will affect the Microsoft Window 95 operating system.
Ping of Death:	It will generate crashes, auto reboot and cause damages to your systems by sending a ping of a certain sizes from a remote machine.
Unauthorized Login Attempt:	It will capture logs whenever an unsuccessful login attempt happens.

General Log 一般系統日誌資訊

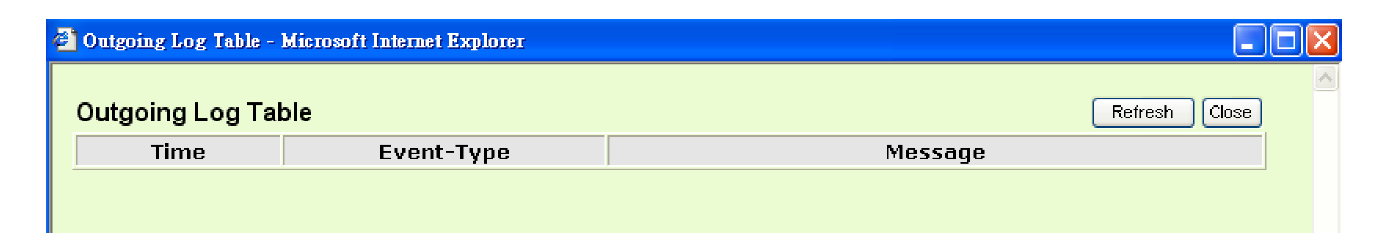
FVR9416 提供了包含以下的一般告警內容訊息,您只要打勾點選即可. 系統錯誤訊息(System Error Messages), 封鎖的政策(Deny Policies), 通過的政策(Allow Policies), 網頁過濾資訊(Content Filtering), Data Inspection, 登入設備(Authorized Login), 設定變更(Configuration Changes).

以下有四個有關線上查詢 **Log** 的按鈕,分別敘述如下:

View System Log: 此為查看系統日誌使用,其資訊內容分別可以於 FVR9416 線上讀取,包含全部-**ALL,** 系統日誌-**System Log,** 封包輸出日誌-**Outgoing Log,** 封包進入日誌-**IncomingLog** 以及 立即清除所有日誌 **Clear Long Now**.如下圖所示:

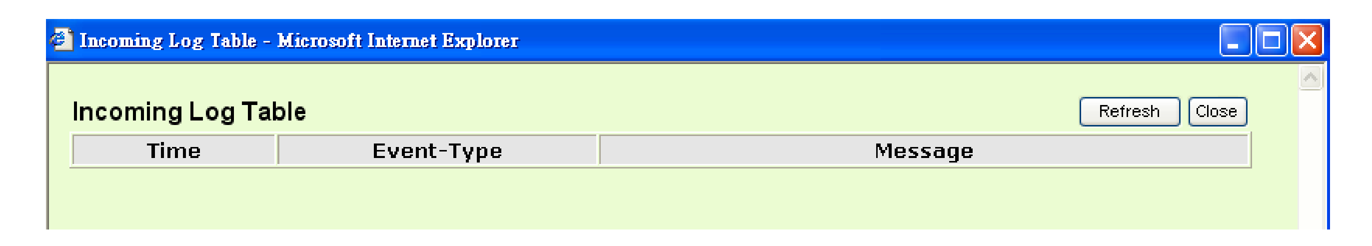


Outgoing Log Table: 查看內部PC出Internet 的系統封包日誌,此日誌內涵內部網路位置(LAN IP), 目的地位置(Destination URL/IP) 以及所使用的通訊服務埠口(Port Number)型態(Type)等信息. 如下圖所示.



Incoming Log Table: 查看外部進入 FVR9416 防火牆的系統封包日誌,此日誌內涵外部來源網路位置(Source IP Address), 目的地位置與通訊埠號(Destination Port Number)等資訊. 如下圖所示.





Clear Log Now: 此按鈕為清除所有目前 FVR9416 的 Log 相關資訊

System Statistics 系統狀態即時監控

Log => System Statistic

Next page >>

Interface	LAN	DMZ	WAN1	WAN2
Device Name	ixp0	ixp5	ixp1	ixp2
Status	Connected	Down	Connected	Down
IP Address	192.168.1.1	0.0.0.0	192.168.5.140	0.0.0.0
MAC Address	00-0c-41-00-00-00	00-0c-41-00-00-05	00-07-40-ca-0b-33	00-0c-41-00-00-02
Subnet Mask	255.255.255.0	0.0.0.0	255.255.255.0	0.0.0.0
Default Gateway	---	0.0.0.0	192.168.5.1	0.0.0.0
DNS	192.168.1.1	---	192.168.5.20 192.168.5.1	0.0.0.0
Received Packets	17911	0	202302	0
Sent Packets	16620	0	19729	0
Total Packets	34531	0	222031	0
Received Bytes	2805045	0	18139722	0
Sent Bytes	8995414	0	6261079	0
Total Bytes	11800459	0	24400801	0
Received Bytes/Sec	0	0	2759	0
Sent Bytes/Sec	0	0	2420	0
Error Packets Received	0	0	0	0
Dropped Packets Received	0	0	0	0
Sessions	---	---	0	0
New Sessions/Sec	---	---	0	0

Refresh

FVR9416 的 **System Statistics** 管理功能可以提供系統目前運作資訊包含 Device Name(機器名稱), Status(目前 WAN 端聯機狀態), IP Address(IP 位置), MAC Address(網路實體位置), Subnet Mask(子網路遮罩), Default Gateway(預設通訊閘), Received Packets(收到的封包數量), Sent Packets(傳送的封包數量), Total Packets(全部的封包數量統計), Received Bytes(收到的封包 Byte 數量統計), Sent Bytes(傳送的封包



Byte 數量統計), Total Bytes(全部的封包 Byte 數量統計), Error Packets Received(收到的錯誤封包統計)以及 Dropped Packets Received(LAN, WAN1 ~ WAN4 丟棄的封包統計)等資訊.

Traffic Statistic:網路流量排名統計

於此畫面可以顯示六種不同的網路流量排名統計,分別解釋如下.

Inbound IP Source Address:進入路由器流量的來源端 IP 地址

于此統計顯示進入路由器來源端 IP 位址的使用流量 bytes/sec 以及百分比例 %.



Traffic Type : Inbound IP Source Address

Source IP	bytes/sec	%
192.168.1.100	4	100

Outbound IP Source Address:從路由器出去流量的來源端 IP 地址

于此統計顯示從路由器出去的來源端 IP 位址的使用流量 bytes/sec 以及百分比例 %..

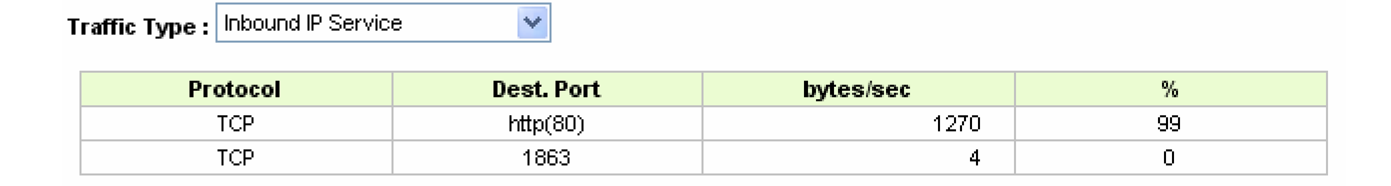


Traffic Type : Outbound IP Source Address

Source IP	bytes/sec	%
192.168.5.173	422	99
192.168.1.100	4	0

Inbound IP Service: 進入路由器流量的服務埠位址

于此統計顯示從路由器進入的通訊服務以及目的埠的使用流量 bytes/sec 以及百分比例 %

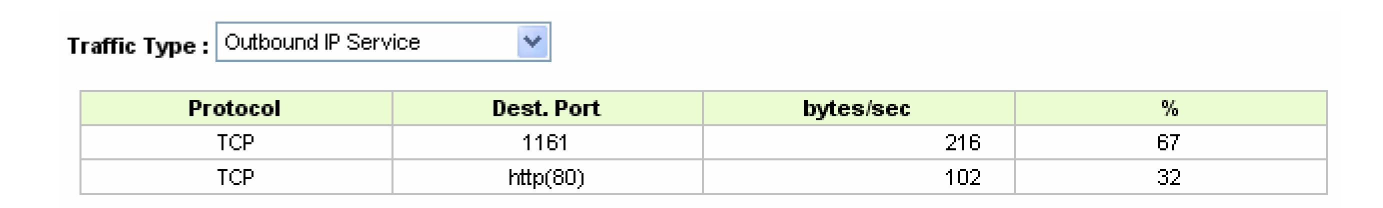


Traffic Type : Inbound IP Service

Protocol	Dest. Port	bytes/sec	%
TCP	http(80)	1270	99
TCP	1863	4	0

Outbound IP Service: 從路由器出去流量的服務埠位址

于此統計顯示從路由器出去的通訊服務以及目的埠的使用流量 bytes/sec 以及百分比例 %.

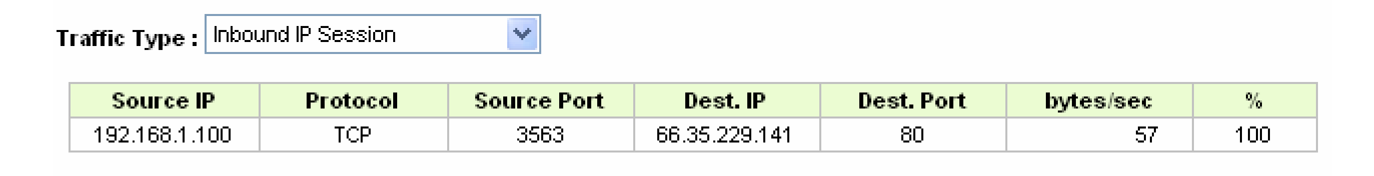


Traffic Type : Outbound IP Service

Protocol	Dest. Port	bytes/sec	%
TCP	1161	216	67
TCP	http(80)	102	32

Inbound IP session: 進入路由器流量的 IP 以及聯線數

于此統計顯示從路由器進入的通訊服務以及來源端 IP 位址,來源端通訊埠,以及目的端 IP 位址與目的端通訊埠的使用流量 bytes/sec 以及百分比例 %.



Traffic Type : Inbound IP Session

Source IP	Protocol	Source Port	Dest. IP	Dest. Port	bytes/sec	%
192.168.1.100	TCP	3563	66.35.229.141	80	57	100

Outbound IP Session: 從路由器出去流量的 IP 以及聯線數

于此統計顯示從路由器出去的通訊服務以及來源端 IP 位址,來源端通訊埠,以及目的端 IP 位址與目的端通訊埠的使用流量 bytes/sec 以及百分比例 %.





Logout



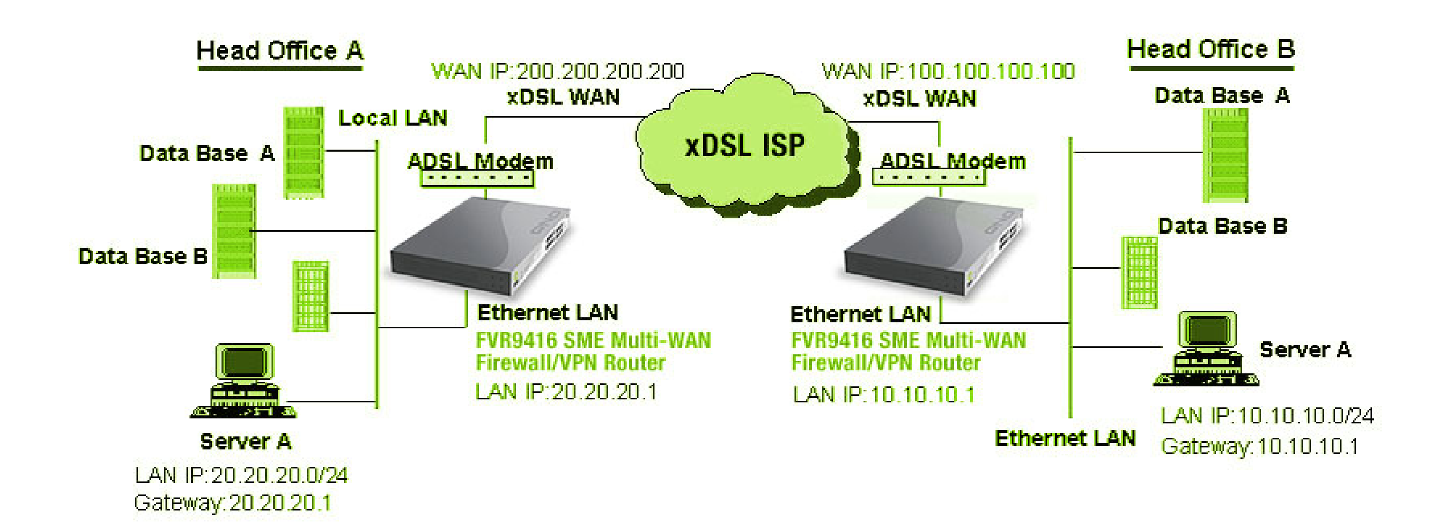
FVR9416 的網頁畫面右下方有一個 **Logout** 的按鈕,此按鈕為終止管理 FVR9416 並登出此管理畫面,若您下次想再進入 FVR9416 管理畫面時,您必須再輸入管理驗證使用名稱與密碼..

5. Troubleshooting

6. FAQ

7. Appendix A: VPN Configuration Sample

Sample VPN Environment 1: Gateway to Gateway



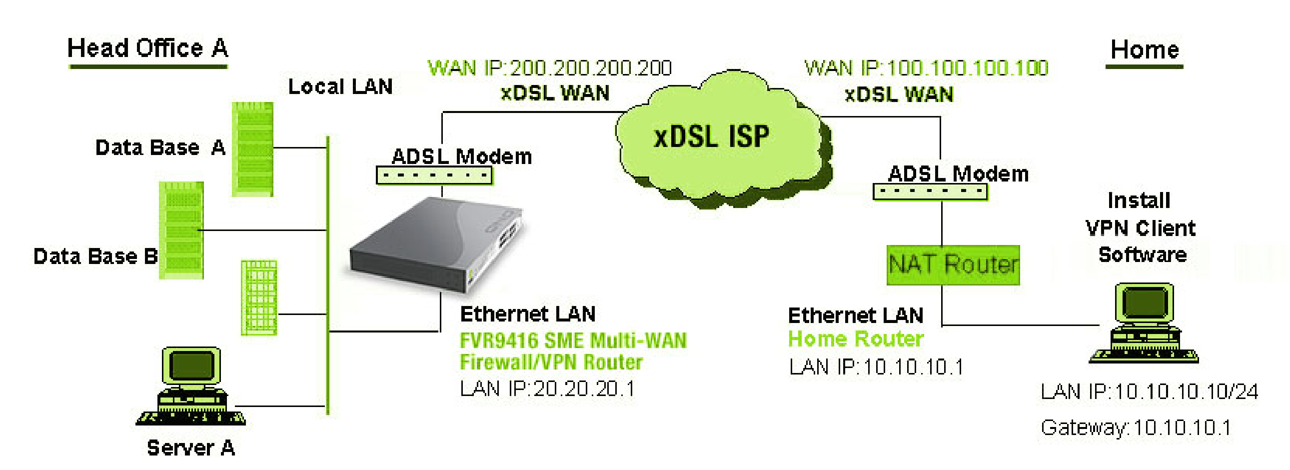


Firewall Setting: Firewall➔General➔Block WAN Request = Disable

VPN Setting: VPN➔Summary➔Add New Tunnel➔Gateway to Gateway

FVR9416 VPN Configuration for	Head Office A	Head Office B
Tunnel Name	HOB	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	Subnet
Local Security Group Type➔ IP Address	20.20.20.0	10.10.10.0
Local Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.0
Remote Security Gateway Type	IP	IP
Remote Security Gateway Type➔ IP Address	100.100.100.100	200.200.200.200
Remote Security Group Type	Subnet	Subnet
Remote Security Group Type➔ IP Address	10.10.10.0	20.20.20.0
Remote Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28,800 Seconds	28,800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Both sides should use the same key.	

Sample VPN Environment 2: Gateway to Gateway



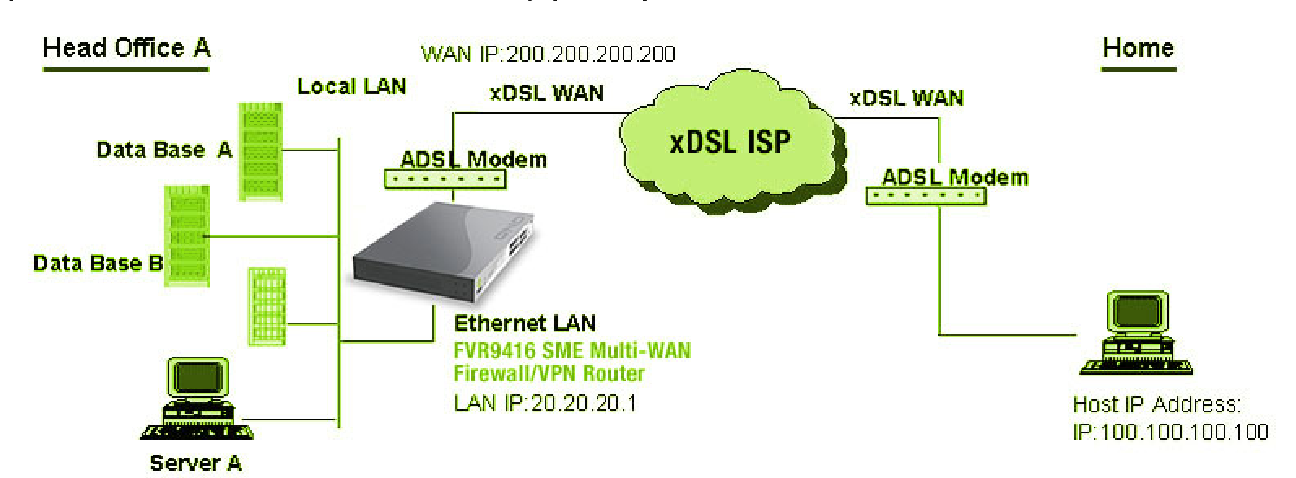
VPN Setting: VPN➔Summary➔Add New Tunnel➔Gateway to Gateway

	Head Office A	Home1 (VPN Client SW)
Tunnel Name	Home1	HOA
Interface	WAN1	WAN



Enable	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type➔ IP Address	20.20.20.0	10.10.10.10
Local Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.0
Remote Security Gateway Type	Domain Name	IP
Remote Security Gateway Type➔ Domain Name	Company domain Name	
Local ID➔ Domain Name		Company domain Name
Remote Security Gateway Type➔ IP Address	100.100.100.100	200.200.200.200
Remote Security Group Type	IP	Subnet
Remote Security Group Type➔ IP Address	10.10.10.10	20.20.20.0
Remote Security Group Type➔ Subnet Mask		255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28,800 Seconds	28,800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	

Sample VPN Environment 3: Client to Gateway (Tunnel)



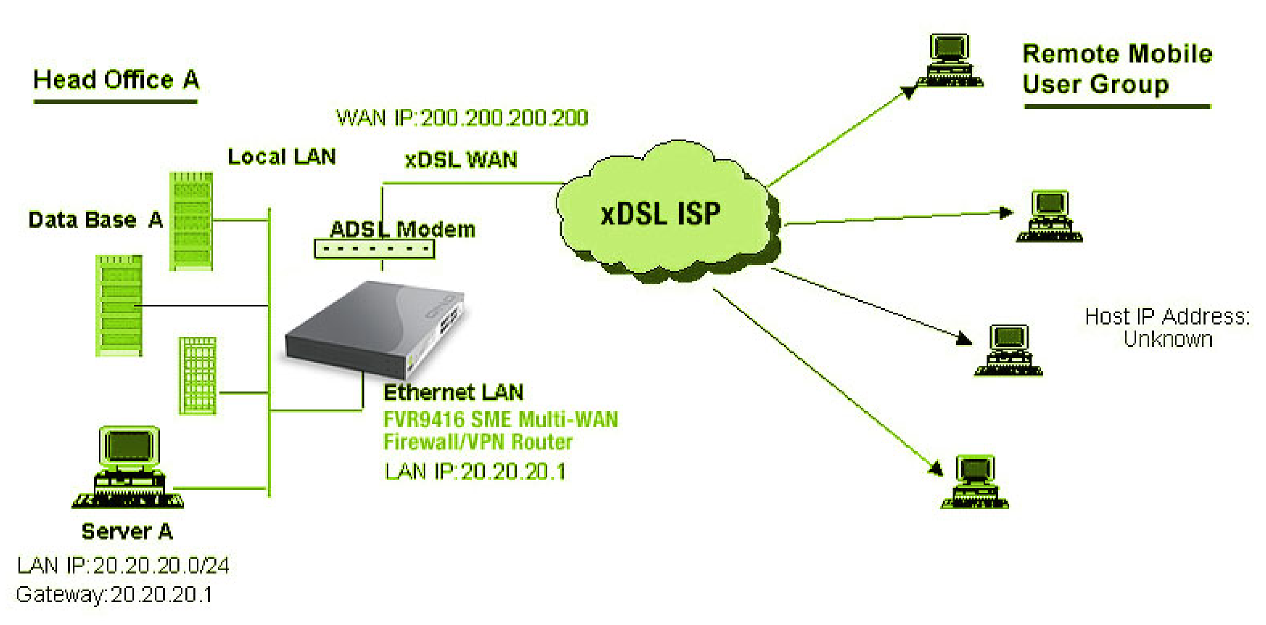
VPN Setting: VPN➔Summary➔Add New Tunnel➔Client to Gateway➔Tunnel

	Head Office A	Home1 (VPN Client SW)
Tunnel Name	Home1	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	IP



Local Security Group Type➔ IP Address	20.20.20.0	100.100.100.100
Local Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.255
Remote Security Gateway Type		IP
Remote Security Gateway Type➔IP Address		200.200.200.200
Remote Client	Email Address	
Remote Client➔ Email Address	User Email Address	
Local ID➔ Email Address		User Email Address
Remote Client➔ IP Address	100.100.100.100	
Remote Security Group Type		Subnet
Remote Security Group Type➔ IP Address		20.20.20.0
Remote Security Group Type➔ Subnet Mask		255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28,800 Seconds	28,800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	

Sample VPN Environment 4: Client to Gateway (GroupVPN)



VPN Setting: VPN➔Summary➔Add New Tunnel➔Client to Gateway➔Group VPN

	Head Office A	Home (VPN Client SW)
Group Name/Tunnel Name	GroupVPN1	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type➔ IP Address	20.20.20.0	Client IP Address
Local Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.255
Remote Security Gateway Type		IP
Remote Security Gateway Type➔IP Address		200.200.200.200
Remote Client	Domain Name	
Remote Client➔ Email Address	Company Domain Name	
Local ID➔ Email Address		Company Domain Name
Remote Security Group Type		Subnet
Remote Security Group Type➔ IP Address		20.20.20.0
Remote Security Group Type➔ Subnet Mask		255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28,800 Seconds	28,800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	
Advanced	Aggressive Mode	

Note: All Clients can sign up into one Group VPN simultaneously